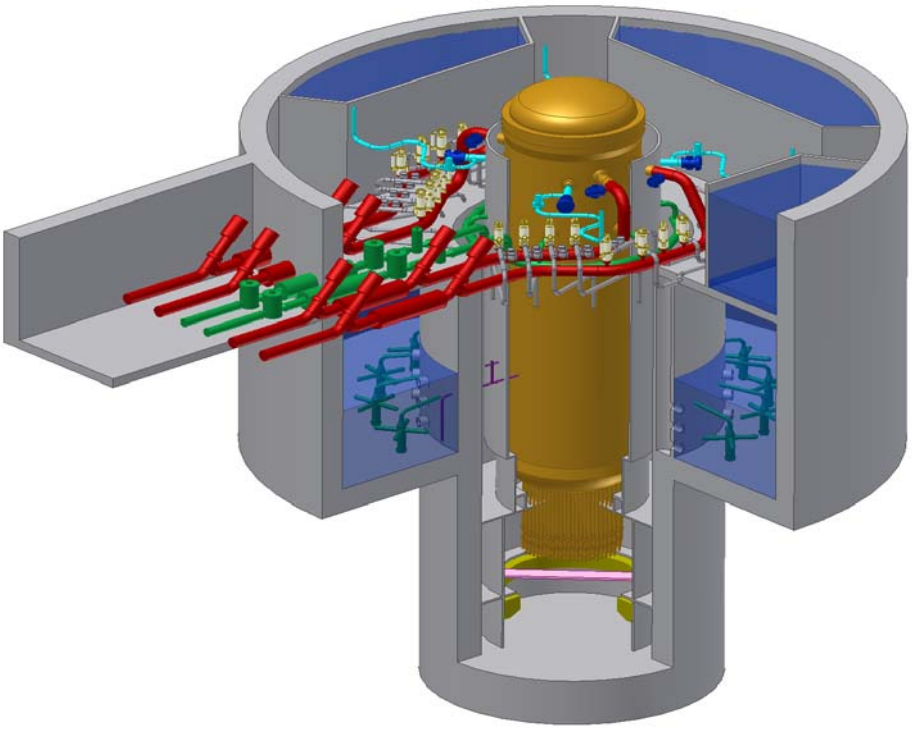
GE Nuclear Energy

26A6642AW
Revision 1
January 2006



ESBWR Design Control Document

Tier 2

Chapter 7

Instrumentation And Control Systems

Contents

List of Tables

List of Illustrations

Abbreviations And Acronyms List

Term	Definition
10 CFR	Title 10, Code of Federal Regulations
A/D	Analog-to-Digital
AASHTO	American Association of Highway and Transportation Officials
AB	Auxiliary Boiler
ABS	Auxiliary Boiler System
ABWR	Advanced Boiling Water Reactor
ac / AC	Alternating Current
AC	Air Conditioning
ACF	Automatic Control Function
ACI	American Concrete Institute
ACS	Atmospheric Control System
AD	Administration Building
ADS	Automatic Depressurization System
AEC	Atomic Energy Commission
AFIP	Automated Fixed In-Core Probe
AGMA	American Gear Manufacturer's Association
AHS	Auxiliary Heat Sink
AHU	Air Handling Units
AISC	American Institute of Steel Construction
AISI	American Iron and Steel Institute
AL	Analytical Limit
ALARA	As Low As Reasonably Achievable
ALWR	Advanced Light Water Reactor
ANS	American Nuclear Society
ANSI	American National Standards Institute
AOO	Anticipated Operational Occurrence
AOV	Air Operated Valve
API	American Petroleum Institute
APRM	Average Power Range Monitor
APR	Automatic Power Regulator
APRS	Automatic Power Regulator System
ARI	Alternate Rod Insertion
ARMS	Area Radiation Monitoring System
ASA	American Standards Association
ASD	Adjustable Speed Drive
ASHRAE	American Society of Heating, Refrigerating, and Air Conditioning Engineers
ASME	American Society of Mechanical Engineers
AST	Alternate Source Term

Abbreviations And Acronyms List

Term	Definition
ASTM	American Society of Testing Methods
AT	Unit Auxiliary Transformer
ATLM	Automated Thermal Limit Monitor
ATWS	Anticipated Transients Without Scram
AV	Allowable Value
AWS	American Welding Society
AWWA	American Water Works Association
B&PV	Boiler and Pressure Vessel
BAF	Bottom of Active Fuel
BHP	Brake Horse Power
BiMAC	Basemat-Internal Melt Arrest Coolability
BOC	Beginning of Cycle
BOP	Balance of Plant
BPU	Bypass Unit
BPV	Bypass Valve
BPWS	Banked Position Withdrawal Sequence
BRE	Battery Room Exhaust
BRL	Background Radiation Level
BTP	NRC Branch Technical Position
BTU	British Thermal Unit
BWR	Boiling Water Reactor
BWROG	Boiling Water Reactor Owners Group
CAV	Cumulative Absolute Velocity
C&FS	Condensate and Feedwater System
C&I	Control and Instrumentation
C/C	Cooling and Cleanup
CB	Control Building
CBGAHVS	Control Building General Area
CBHVAC	Control Building HVAC
CBHVS	Control Building Heating, Ventilation and Air Conditioning System
CCI	Core-Concrete Interaction
CDF	Core Damage Frequency
CDU	Condensing Unit
CFR	Code of Federal Regulations
CH	Chugging
CIRC	Circulating Water System
CIS	Containment Inerting System
CIV	Combined Intermediate Valve
CLAVS	Clean Area Ventilation Subsystem of Reactor Building HVAC

Abbreviations And Acronyms List

Term	Definition
CM	Cold Machine Shop
CMS	Containment Monitoring System
CMU	Control Room Multiplexing Unit
CO	Condensate Oscillation
COL	Combined Operating License
COLR	Core Operating Limits Report
CONAVS	Controlled Area Ventilation Subsystem of Reactor Building HVAC
CPR	Critical Power Ratio
CPS	Condensate Purification System
CPU	Central Processing Unit
CR	Control Rod
CRD	Control Rod Drive
CRDA	Control Rod Drop Accident
CRDH	Control Rod Drive Housing
CRDHS	Control Rod Drive Hydraulic System
CRDS	Control Rod Drive System
CRGT	Control Rod Guide Tube
CRHA	Control Room Habitability Area
CRHAHVS	Control Room Habitability Area HVAC Sub-system
CRT	Cathode Ray Tube
CS&TS	Condensate Storage and Transfer System
CSDM	Cold Shutdown Margin
CS / CST	Condensate Storage Tank
CT	Main Cooling Tower
CTVCF	Constant Voltage Constant Frequency
CUF	Cumulative usage factor
CWS	Chilled Water System
D-RAP	Design Reliability Assurance Program
DAC	Design Acceptance Criteria
DAW	Dry Active Waste
DBA	Design Basis Accident
DBE	Design Basis Event
DB%	Dry-Basis-Percent
dc / DC	Direct Current
DCD	Design Control Document
DCS	Drywell Cooling System
DCIS	Distributed Control and Information System
DEPSS	Drywell Equipment and Pipe Support Structure
DF	Decontamination Factor

Abbreviations And Acronyms List

Term	Definition
D/F	Diaphragm Floor
DG	Diesel-Generator
DHR	Decay Heat Removal
DPS	Diverse Protection System
DM&C	Digital Measurement and Control
DOF	Degree of Freedom
DOI	Dedicated Operators Interface
DORT	Discrete Ordinates Techniques
DOT	Department of Transportation
dPT	Differential Pressure Transmitter
DPS	Diverse Protection System
DPV	Depressurization Valve
DR&T	Design Review and Testing
DTM	Digital Trip Module
DW	Drywell
EAB	Exclusion Area Boundary
EB	Electrical Building
EBAS	Emergency Breathing Air System
EBHV	Electrical Building HVAC
ECCS	Emergency Core Cooling System
E-DCIS	Essential DCIS (Distributed Control and Information System)
EDO	Environmental Qualification Document
EFDS	Equipment and Floor Drainage System
EFPY	Effective Full Power Years
EFU	Emergency Filter Unit
EHC	Electro-Hydraulic Control (Pressure Regulator)
ENS	Emergency Notification System
EOC	Emergency Operations Center
EOC	End of Cycle
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedures
EPDS	Electric Power Distribution System
EPG	Emergency Procedure Guidelines
EPRI	Electric Power Research Institute
EQ	Environmental Qualification
ERICP	Emergency Rod Insertion Control Panel
ERIP	Emergency Rod Insertion Panel
ESF	Engineered Safety Feature
ESP	Early Site Permit

Abbreviations And Acronyms List

Term	Definition
ETS	Emergency Trip System
FAC	Flow-Accelerated Corrosion
FAPCS	Fuel and Auxiliary Pools Cooling System
FATT	Fracture Appearance Transition Temperature
FB	Fuel Building
FBHV	Fuel Building HVAC
FCI	Fuel-Coolant Interaction
FCISL	Fuel Cladding Integrity Safety Limit
FCM	File Control Module
FCS	Flammability Control System
FCU	Fan Cooling Unit
FDDI	Fiber Distributed Data Interface
FEBAVS	Fuel Building Ventilation System
FFT	Fast Fourier Transform
FFWTR	Final Feedwater Temperature Reduction
FHA	Fire Hazards Analysis
FHA	Fuel Handling Accident
FIV	Flow-Induced Vibration
FMCRD	Fine Motion Control Rod Drive
FMEA	Failure Modes and Effects Analysis
FPS	Fire Protection System
FO	Diesel Fuel Oil Storage Tank
FOAKE	First-of-a-Kind Engineering
FPC	Fuel Pool Cleanup
FPE	Fire Pump Enclosure
FS	Partial Full Scale
FSI	Fluid Structure Interaction
FTDC	Fault-Tolerant Digital Controller
FW	Feedwater
FWCS	Feedwater Control System
FWLB	Feedwater Line Break
FWS	Fire Water Storage Tank
GCS	Generator Cooling System
GDC	General Design Criteria
GDCS	Gravity-Driven Cooling System
GE	General Electric Company
GENE	GE Nuclear Energy
GEN	Main Generator System
GETAB	General Electric Thermal Analysis Basis

Abbreviations And Acronyms List

Term	Definition
GL	Generic Letter
GM	Geiger-Mueller Counter
GM-B	Beta-Sensitive GM (Geiger-Mueller Counter) Detector
GENE	General Electric Nuclear Energy
GNF	Global Nuclear Fuel
GSIC	Gamma-Sensitive Ion Chamber
GSOS	Generator Sealing Oil System
GWSR	Ganged Withdrawal Sequence Restriction
HAZ	Heat-Affected Zone
HCU	Hydraulic Control Unit
HCW	High Conductivity Waste
HDVS	Heater Drain and Vent System
HEI	Heat Exchange Institute
HELB	High Energy Line Break
HELSA	High Energy Line Separation Analysis
HEP	Human Error Probability
HEPA	High Efficiency Particulate Air/Absolute
HFE	Human Factors Engineering
HFF	Hollow Fiber Filter
HGCS	Hydrogen Gas Cooling System
HIC	High Integrity Container
HID	High Intensity Discharge
HIS	Hydraulic Institute Standards
HM	Hot Machine Shop & Storage
HP	High Pressure
HPNSS	High Pressure Nitrogen Supply System
HPT	High-Pressure Turbine
HRA	Human Reliability Assessment
HSI	Human-System Interface
HSSS	Hardware/Software System Specification
HVAC	Heating, Ventilation and Air Conditioning
HVS	High Velocity Separator
HVT	Horizontal Vent Test
HWC	Hydrogen Water Chemistry
HWCS	Hydrogen Water Chemistry System
HWS	Hot Water System
HX	Heat Exchanger
I&C	Instrumentation and Control
I/O	Input/Output

Abbreviations And Acronyms List

Term	Definition
IAS	Instrument Air System
IASCC	Irradiation Assisted Stress Corrosion Cracking
IBA	Intermediate Break Accident
IBC	International Building Code
IC	Ion Chamber
IC	Isolation Condenser
ICD	Interface Control Diagram
ICP	Instrument and Control Power
ICPR	Initial Critical Power Ratio
ICS	Isolation Condenser System
IE	Inspection and Enforcement
IEB	Inspection and Enforcement Bulletin
IED	Instrument and Electrical Diagram
IEEE	Institute of Electrical and Electronic Engineers
IFTS	Inclined Fuel Transfer System
IGSCC	Intergranular Stress Corrosion Cracking
IIS	Iron Injection System
ILRT	Integrated Leak Rate Test
IOP	Integrated Operating Procedure
IMC	Induction Motor Controller
IMCC	Induction Motor Controller Cabinet
IRM	Intermediate Range Monitor
ISA	Instrument Society of America
ISI	In-Service Inspection
ISLT	In-Service Leak Test
ISM	Independent Support Motion
ISMA	Independent Support Motion Response Spectrum Analysis
ISO	International Standards Organization
ITA	Inspections, Tests or Analyses
ITAAC	Inspections, Tests, Analyses and Acceptance Criteria
ITA	Initial Test Program
LAPP	Loss of Alternate Preferred Power
LBB	Leak Before Break
LCO	Limiting Conditions for Operation
LCW	Low Conductivity Waste
LD	Logic Diagram
LDA	Lay down Area
LDW	Lower Drywell
LD&IS	Leak Detection and Isolation System

Abbreviations And Acronyms List

Term	Definition
LED	Light Emitting Diode
LERF	Large Early Release Frequency
LFCV	Low Flow Control Valve
LHGR	Linear Heat Generation Rate
LLRT	Local Leak Rate Test
LMU	Local Multiplexer Unit
LO	Dirty/Clean Lube Oil Storage Tank
LOCA	Loss-of-Coolant-Accident
LOFW	Loss-of-feedwater
LOOP	Loss of Offsite Power
LOPP	Loss of Preferred Power
LP	Low Pressure
LPCI	Low Pressure Coolant Injection
LPCRD	Locking Piston Control Rod Drive
LPMS	Loose Parts Monitoring System
LPRM	Local Power Range Monitor
LPSP	Low Power Setpoint
LUA	Lead Use Assembly
LWMS	Liquid Waste Management System
MAAP	Modular Accident Analysis Program
MAPLHGR	Maximum Average Planar Linear Head Generation Rate
MAPRAT	Maximum Average Planar Ratio
MBB	Motor Built-In Brake
MCC	Motor Control Center
MCES	Main Condenser Evacuation System
MCOP	Manual containment overpressure protection (function)
MCPR	Minimum Critical Power Ratio
MCR	Main Control Room
MCRP	Main Control Room Panel
MELB	Moderate Energy Line Break
MLHGR	Maximum Linear Heat Generation Rate
MMI	Man-Machine Interface
MMIS	Man-Machine Interface Systems
MOV	Motor-Operated Valve
MPC	Maximum Permissible Concentration
MPL	Master Parts List
MRBM	Multi-Channel Rod Block Monitor
MS	Main Steam
MSIV	Main Steam Isolation Valve

Abbreviations And Acronyms List

Term	Definition
MSL	Main Steamline
MSLB	Main Steamline Break
MSLBA	Main Steamline Break Accident
MSR	Moisture Separator Reheater
MSV	Mean Square Voltage
MT	Main Transformer
MTTR	Mean Time To Repair
MWS	Makeup Water System
NBR	Nuclear Boiler Rated
NBS	Nuclear Boiler System
NCIG	Nuclear Construction Issues Group
NDE	Nondestructive Examination
NE-DCIS	Non-Essential Distributed Control and Information System
NDRC	National Defense Research Committee
NDT	Nil Ductility Temperature
NFPA	National Fire Protection Association
NIST	National Institute of Standard Technology
NICWS	Nuclear Island Chilled Water Subsystem
NMS	Neutron Monitoring System
NOV	Nitrogen Operated Valve
NPHS	Normal Power Heat Sink
NPSH	Net Positive Suction Head
NRC	Nuclear Regulatory Commission
NRHX	Non-Regenerative Heat Exchanger
NS	Non-seismic
NSSS	Nuclear Steam Supply System
NT	Nitrogen Storage Tank
NTSP	Nominal Trip Setpoint
O&M	Operation and Maintenance
O-RAP	Operational Reliability Assurance Program
OBCV	Overboard Control Valve
OBE	Operating Basis Earthquake
OGS	Offgas System
OHLHS	Overhead Heavy Load Handling System
OIS	Oxygen Injection System
OLMCPR	Operating Limit Minimum Critical Power Ratio
OLU	Output Logic Unit
OOS	Out-of-Service
ORNL	Oak Ridge National Laboratory

Abbreviations And Acronyms List

Term	Definition
OSC	Operational Support Center
OSHA	Occupational Safety and Health Administration
OSI	Open Systems Interconnect
P&ID	Piping and Instrumentation Diagram
PA/PL	Page/Party-Line
PABX	Private Automatic Branch (Telephone) Exchange
PAM	Post Accident Monitoring
PAR	Passive Autocatalytic Recombiner
PAS	Plant Automation System
PASS	Post Accident Sampling Subsystem of Containment Monitoring System
PCC	Passive Containment Cooling
PCCS	Passive Containment Cooling System
PCT	Peak Cladding Temperature
PCV	Primary Containment Vessel
PDA	Piping Design Analysis
PFD	Process Flow Diagram
PGA	Peak Ground Acceleration
PGCS	Power Generation and Control Subsystem of Plant Automation System
PH	Pump House
PL	Parking Lot
PM	Preventive Maintenance
PMCS	Performance Monitoring and Control Subsystem of NE-DCIS
PMF	Probable Maximum Flood
PMP	Probable Maximum Precipitation
PQCL	Product Quality Check List
PRA	Probabilistic Risk Assessment
PRMS	Process Radiation Monitoring System
PRNM	Power Range Neutron Monitoring
PS	Plant Stack or Pool Swell
PSD	Power Spectral Density
PSS	Process Sampling System
PSTF	Pressure Suppression Test Facility
PSWS	Plant Service Water System
PT	Pressure Transmitter
PWR	Pressurized Water Reactor
QA	Quality Assurance
RACS	Rod Action Control Subsystem
RAM	Reliability, Availability and Maintainability
RAPI	Rod Action and Position Information

Abbreviations And Acronyms List

Term	Definition
RAT	Reserve Auxiliary Transformer
RB	Reactor Building
RBC	Rod Brake Controller
RBCC	Rod Brake Controller Cabinet
RBCWS	Reactor Building Chilled Water Subsystem
RBHV	Reactor Building HVAC (Heating, Ventilation and Air Conditioning)
RBS	Rod Block Setpoint
RBV	Reactor Building Vibration
RC&IS	Rod Control and Information System
RCC	Remote Communication Cabinet
RCCV	Reinforced Concrete Containment Vessel
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary
RCS	Reactor Coolant System
RDA	Rod Drop Accident
RDC	Resolver-to-Digital Converter
REPAVS	Refueling and Pool Area Ventilation Subsystem of Fuel Building HVAC (Heating, Ventilation and Air Conditioning)
RFP	Reactor Feed Pump
RG	Regulatory Guide
RHR	Residual Heat Removal (function)
RHX	Regenerative Heat Exchanger
RMS	Root Mean Square
RMS	Radiation Monitoring Subsystem
RLP	Reference Loading Pattern
RMU	Remote Multiplexer Unit
RO	Reverse Osmosis
ROM	Read-only Memory
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RRPS	Reference Rod Pull Sequence
RSM	Rod Server Module
RSPC	Rod Server Processing Channel
RSS	Remote Shutdown System
RSSM	Reed Switch Sensor Module
RSW	Reactor Shield Wall
RTIF	Reactor Trip and Isolation Function(s)
RT_{NDT}	Reference Temperature of Nil-Ductility Transition
RTP	Reactor Thermal Power
RW	Radwaste Building

Abbreviations And Acronyms List

Term	Definition
RWBCR	Radwaste Building Control Room
RWBGA	Radwaste Building General Area
RWBHVAC	Radwaste Building HVAC (Heating, Ventilation and Air Conditioning)
RWCU/SDC	Reactor Water Cleanup/Shutdown Cooling
RWE	Rod Withdrawal Error
RWM	Rod Worth Minimizer
SA	Severe Accident
SAM	Severe Accident Management
SAR	Safety Analysis Report
SB	Service Building
SBA	Small Break Accident
S/C	Digital Gamma-Sensitive GM (Geiger-Mueller Counter) Detector
SC	Suppression Chamber
S/D	Scintillation Detector
S/DRSRO	Single/Dual Rod Sequence Restriction Override
S/N	Signal-to-Noise
S/P	Suppression Pool
SAS	Service Air System
SB&PC	Steam Bypass and Pressure Control System
SBO	Station Blackout
SBWR	Simplified Boiling Water Reactor
SCEW	System Component Evaluation Work
SCRRI	Selected Control Rod Run-in
SDC	Shutdown Cooling
SDM	Shutdown Margin
SDS	System Design Specification
SEOA	Sealed Emergency Operating Area
SER	Safety Evaluation Report
SF	Service Water Building
SFA	Spent Fuel Assembly
SFP	Spent fuel pool
SIL	Service Information Letter
SIT	Structural Integrity Test
SIU	Signal Interface Unit
SJAE	Steam Jet Air Ejector
SLC	Standby Liquid Control
SLMCPR	Safety Limit Minimum Critical Power Ratio
SMU	SSLC (Safety System Logic and Control) Multiplexing Unit
SOV	Solenoid Operated Valve

Abbreviations And Acronyms List

Term	Definition
SP	Setpoint
SPC	Suppression Pool Cooling
SPDS	Safety Parameter Display System
SPTMS	Suppression Pool Temperature Monitoring Subsystem of Containment Monitoring System
SR	Surveillance Requirement
SRM	Source Range Monitor
SRNM	Startup Range Neutron Monitor
SRO	Senior Reactor Operator
SRP	Standard Review Plan
SRS	Software Requirements Specification
SRSRO	Single Rod Sequence Restriction Override
SRSS	Square Root Sum of Squares
SRV	Safety Relief Valve
SRVDL	Safety Relief Valve Discharge Line
SSAR	Standard Safety Analysis Report
SS	Sub-scale
SST	Sub-scale Test
SSC(s)	Structure, System and Component(s)
SSE	Safe Shutdown Earthquake
SSI	Soil Structure Interaction
SSLC	Safety System Logic and Control
SSPC	Steel Structures Painting Council
ST	Spare Transformer
STI	Startup Test Instruction
STP	Sewage Treatment Plant
STRAP	Scram Time Recording and Analysis Panel
STRP	Scram Time Recording Panel
SV	Safety Valve
SWH	Static Water Head
SWMS	Solid Waste Management System
SY	Switch Yard
TAF	Top of Active Fuel
TASS	Turbine Auxiliary Steam System
TB	Turbine Building
TBCE	Turbine Building Compartment Exhaust
TBAS	Turbine Building Air Supply
TBE	Turbine Building Exhaust
TBLOE	Turbine Building Lube Oil Area Exhaust
TBS	Turbine Bypass System

Abbreviations And Acronyms List

Term	Definition
TBHV	Turbine Building HVAC (Heating, Ventilation and Air Conditioning)
TBV	Turbine Bypass Valve
TC	Training Center
TCCWS	Turbine Component Cooling Water System
TCS	Turbine Control System
TCV	Turbine Control Valve
TDH	Total Developed Head
TEDE	Total Effective Dose Equivalent
TEMA	Tubular Exchanger Manufacturers' Association
TFSP	Turbine First Stage Pressure
TG	Turbine Generator
TGSS	Turbine Gland Seal System
THA	Time-History Accelerograph
TIP	Traversing In-core Probe
TLOS	Turbine Lubricating Oil System
TLU	Trip Logic Unit
TMI	Three Mile Island
TMSS	Turbine Main Steam System
TRAC	Transient Reactor Analysis Code
TRM	Technical Requirements Manual
TS	Technical Specification(s)
TSC	Technical Support Center
TSI	Turbine Supervisory Instrument
TSV	Turbine Stop Valve
TTWFATBV	Turbine trip with failure of all bypass valves
UBC	Uniform Building Code
UHS	Ultimate Heat Sink
UL	Underwriter's Laboratories Inc.
UPS	Uninterruptible Power Supply
URD	Utilities Requirements Document
USE	Upper Shelf Energy
USM	Uniform Support Motion
USMA	Uniform Support Motion Response Spectrum Analysis
USNRC	United States Nuclear Regulatory Commission
USS	United States Standard
UV	Ultraviolet
V&V	Verification and Validation
Vac / VAC	Volts Alternating Current
Vdc / VDC	Volts Direct Current

Abbreviations And Acronyms List

Term	Definition
VDU	Video Display Unit
VW	Vent Wall
VWO	Valves Wide Open
WD	Wash Down Bays
WH	Warehouse
WS	Water Storage
WT	Water Treatment
WW	Wetwell
XMFR	Transformer
ZPA	Zero Period Acceleration

7. INSTRUMENTATION AND CONTROL SYSTEMS

7.1 INTRODUCTION

This chapter presents the specific detailed design and performance information relative to the instrumentation and control (I&C) aspects of safety-related and nonsafety-related systems (which are important for plant operation) utilized throughout the plant. Many of the systems have other design aspects relative to mechanical, radiological, and other items that are described in other chapters.

7.1.1 Identification of I&C Systems

7.1.1.1 General

Instrumentation and control systems are designated as either nonsafety-related systems or safety-related systems, depending on their functions. Some portions of a system may have a safety function, while other portions of the same system may be classified as nonsafety-related. A description of the system of classification can be found in Section 3.2.

Because the ESBWR safety-related functions (including engineered safety features) do not rely on diesel-generator backed electrical energy or active systems by design, the necessary safety-related instruments and controls are considerably reduced and simplified compared to previous BWR plant designs. The systems presented in Chapter 7 are arranged consistent with the Nuclear Regulatory Commission (NRC) Standard Review Plan (SRP), Reference 7.1-1, with slight variations in some section titles to accommodate ESBWR design philosophy, i.e., Introduction, Reactor Trip System, Engineered Safety Feature (ESF) Systems, Shutdown Systems, Safety-Related and Nonsafety-related Information Systems, Interlock Systems, Control Systems, Diverse Instrumentation and Controls, and Data Communication Systems. Table 7.1-1 shows the application of the regulatory requirements specified in the SRP to the various systems.

Each individual safety-related system utilizes redundant channels of safety-related instruments for initiating safety action. The automatic decision-making and trip logic functions associated with the safety actions of the safety-related reactor trip system and engineered safety feature systems are accomplished by a four-division, separated protection logic system framework called the Safety System Logic and Control (SSLC). The SSLC provides the hardware and software platforms for the logic for the safety-related protection functions, such as reactor trip, isolation, and emergency core cooling functions. The SSLC multi-divisional system includes divisionally separate panels which house the SSLC equipment for controlling the various safety functions and the actuation devices. The SSLC receives input signals from the redundant channels of safety-related instrumentation, and uses the input information to perform logic functions in making decisions for safety actions. The ESBWR systems, which have logic implemented in the SSLC, include the Reactor Protection (Trip) System, the Suppression Pool Temperature Monitoring function of the Containment Monitoring System, the control logic of the Automatic Depressurization System of the Nuclear Boiler System, the control logic of the Gravity-Driven Cooling System, the Leak Detection and Isolation System, and the control logic of the Isolation Condenser System. Divisional separation is also applied to the Essential Distributed Control and Information System (E-DCIS), which provides data highways for the sensor input to the logic units and for the logic output to the system actuators (actuated devices such as valves or squibs).

These and other SSLC interfaces are identified in the following subsections, and discussed in detail in the appropriate sections of this chapter. A simplified block diagram showing the major ESBWR I&C systems and main control room interfaces is shown in Figure 7.1-1.

Note that the ESBWR instrumentation and control (I&C) systems provide many levels of diversity. In general the RPS and MSIV isolation use separate sensors, hardware and software than the ESF I&C. Furthermore, ATWS/SLC system is implemented in non-microprocessor based hardware and uses separate level transmitters than RPS. A diverse protection system, which includes both diverse RPS and diverse ESF actuation functions using different sensors, hardware and software platforms than either of the safety related I&C systems is also provided. Finally the nonsafety related I&C systems which operate both plant investment protection (PIP) systems and BOP systems are also different hardware and software platforms than the safety I&C systems. Figure 7.1-2 presents a block diagram identifying the diverse hardware and software platforms of the ESBWR I&C systems.

7.1.1.2 The ESBWR Instrumentation and Control Architecture

The ESBWR instrumentation and control (I&C) systems consist of both safety-related and nonsafety-related control systems. The primary safety-related systems, such as the Reactor Protection System (RPS), Leak Detection and Isolation System (LD&IS), and the ESF initiation logics, are encompassed by the Safety System Logic and Control (SSLC) framework. The SSLC and safety-related systems are supported by the safety-related data communication network, the Essential Distributed Control and Information System (E-DCIS). The nonsafety-related (control) systems include all other plant I&C systems, which are supported by the nonsafety-related data communication network, the Non-Essential Distributed Control and Information System (NE-DCIS). A simplified block diagram of the ESBWR I&C architecture is shown in Figure 7.1-1.

7.1.1.2.1 The Safety System Logic and Control (SSLC) Architecture

The safety-related I&C systems consists of the SSLC and other individual monitoring systems such as the Neutron Monitoring System and the Process Radiation Monitoring System, etc. The SSLC is a four-division, separate and redundant protection logic system framework that provides automatic decision-making and trip logic functions to implement the safety actions of the safety-related reactor trip system and engineered safety feature systems within the framework. The SSLC multi-divisional system includes divisionally separate panels which house the SSLC equipment for controlling the various safety functions and the actuation devices. Figure 7.3-5 provides an overview of the structure of the SSLC, which mainly consists of the Reactor Trip and Isolation Function (RTIF) part of the framework and the Engineering Safety Features (ESF) part of the framework. The RTIF includes the logics of the Reactor Protection System (RPS) for reactor scram and the isolation logics of main steam-line isolation valves (MSIV). The ESF logics include all ECCS initiation logics for the opening of Automatic Depressurization System (ADS) Safety Relief Valves (SRV), Depressurization Valves (DPV), Gravity-Driven Cooling System (GDCS) squib valves, and Isolation Condenser (IC) valves. It also includes the LD&IS logics and the Standby Liquid Control System liquid boron injection initiation logic for the Anticipated Transient Without Scram (ATWS) function.

SSLC/RTIF

The basic system architecture of the RTIF, i.e., the RPS and MSIV Isolation part of SSLC, employs four independent trip logic systems in four separate divisions of safety protection equipment, as shown in Figure 7.2-1. The four redundant RPS divisions are identical in design and independent in operation. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. The logic in each division does not depend on time-of-day and is asynchronous to the other divisions; no division depends on the correct operation of another division nor on interdivisional communication links. As shown in Figure 7.2-1, each division has the Remote Multiplexing Unit (RMU) function, the Digital Trip Module (DTM) function, the Trip Logic Unit (TLU) function, the Output Logic Unit (OLU) function, and the Communication Interface Module (CIM) function. The RMU receives input from the sensors device and performs analog-to-digital conversion and signal processing function. The digitized signal is then sent to the DTM. Some signals are directly sent to the DTM such as those from the turbine stop valves and control valves positions. The DTM generates the trip signal to the TLU based on setpoint comparison. The DTM and the TLU reside in separate and independent processors. Each TLU receives the trip status from the DTMs in all four divisions and perform 2 out of 4 logic to determine the trip status for each system. Some trip signals are sent to the TLU directly from other inputs such as the NMS trip signals and operator manual inputs. The DTM receives division of sensor bypass signal to activate divisional trip bypass. The trip signal from the TLU is then sent to the OLU in this division and output to the load drivers in the scram circuitry. The CIM serves as the communication interface for data communication between the RTIF division and the nonsafety systems. The RPS logic and system design arrangement and architecture are described in more detail in Subsection 7.2.1.2.4. Like the ABWR, the ESBWR RPS logic will scram the plant when any two or more same parameters (in two or more divisions) exceed their trip value, under any single failure and any division of sensors/logic bypass.

For the actual hardware and software design platform descriptions of the RTIF, detailed information of the platform concept is included in the referenced documents. Reference 7.1-2 provides a sample description of the platform performance of various functional components in RTIF applied in ABWR. The ESBWR employs the same functional components and platform structure. Reference 7.1-3 provides a sample detailed hardware and software functional description and specification of the RTIF applied in ABWR. Such RTIF hardware and software platform structure concept is identical to that of ESBWR. To provide as an example of a key RTIF component, Reference 7.1-4 provides the sample software design description and specification of the Digital Trip Module (DTM) of the RTIF applied in ABWR. Such RTIF DTM component structure concept is identical to that of ESBWR. In addition, Reference 7.1-5 and Reference 7.1-6 also provide the typical safety-related NMS system component units platform concepts (PRNM and SRNM) that are identical to that used in ESBWR NMS. Other than detailed specific parameters application and logic hardware/software designs, the ESBWR SSLC/RTIF architecture concept is identical to that of the ABWR. The ABWR SSLC/RTIF architecture concept has been reviewed and approved per the ABWR Certification.

SSLC/ESF

The ESF part of SSLC also follows a four-division architecture and platform. The basic system architecture of the ESF logics employs four independent trip logic systems in four separate

divisions of safety protection equipment, as shown in Figure 7.3-4. The four redundant ESF logic divisions are identical in design and independent in operation. There are four instrument channels for each ESF logic division. Four sensors, one per division, are provided for each variable monitored. The logic data in each division does not depend on time-of-day and is asynchronous to the other divisions; no division depends on the correct operation of another division nor on interdivisional communication links. The ESF logic design arrangement and architecture are described in more details in Subsection 7.3.4.2. SSLC/ESF input data (process variables) are multiplexed via the Essential DCIS (E-DCIS) in four physically and electrically isolated redundant divisions. Each of the four independent and separated E-DCIS channels feeds separate and independent channel of SSLC/ESF equipment.

As shown in Figure 7.3-4, each division of ESF logic has the Remote Multiplexing Unit (RMU), the Digital Trip Module (DTM) function, the Voter Logic Unit (VLU) function, the Network Interface Module (NIM) function and Communication Interface Module (CIM) function, and the Bridge Transfer Module (BTM) function. It also contains the safety-related visual display unit (VDU) for operator interface. Either directly or via data link, all the units within the network are connected by redundant fiber optic ring type network. The RMU is the input/output device and used either for sensor input function or for signal output function to actuators. The DTM generates the trip signal to the VLU based on setpoint comparison. The VLU and the DTM reside in separate and independent processors. The VLU is a dual logic function unit that processes two independent logic paths. Each VLU receives the trip status from the DTMs in all four divisions and perform 2-out-of-4 logic, in both logic paths independently, to determine the trip status for each system. The CIM serves as the communication interface for data communication between different ESF divisions and between the ESF division and other safety-related signal inputs from RPS and NMS. The BTM is used as the interface and isolation device to transfer data from the ESF division to nonsafety network through a gateway. Data is received at the input module of the RMU and processed in the RMU. It is then sent to the DTM for setpoint comparison. The resulted signal from this division and other three divisions are then processed by the VLU for 2-out-of-4 trip decision. The trip signal is then sent to the output RMU in all four divisions. The data is then sent by hardwire from the RMU to equipment for actuation. The safety-related VDU provides the operator with display and control interfaces. Specific descriptions of the SSLC/ESF logic function is presented in Subsection 7.3.4.2. Other than detailed specific parameters application and logic hardware/software designs, the ESBWR SSLC/ESF architecture concept is identical to that of the ABWR. The ABWR SSLC/ESF architecture concept has been reviewed and approved per the ABWR Certification[FCC3].

7.1.1.3 Reactor Trip System

Reactor Protection System (RPS)

The safety-related RPS I&C initiates an automatic reactor shutdown by rapid insertion of control rods (scram) if monitored system variables exceed pre-established limits. This action prevents fuel damage, limits system pressure and thus restricts the release of radioactive material.

Neutron Monitoring System (NMS)

The safety-related NMS monitors the core neutron flux from the startup source range to beyond rated power. The NMS provides logic signals to the RPS to automatically shut down the reactor

when a condition necessitating a reactor scram is detected. The NMS is composed of four subsystems:

- Startup range neutron monitor (SRNM);
- Power range neutron monitor (PRNM), a subsystem that includes the local power range monitor (LPRM), the average power range monitor (APRM), and the oscillation power range monitor (OPRM) functions;
- Automatic fixed in-core probe (AFIP) (nonsafety-related; refer to Subsection 7.1.1.8.); and
- Multi-Channel Rod Block Monitor (MRBM) (nonsafety-related; refer to Subsection 7.1.1.8.).

Suppression Pool Temperature Monitoring Subsystem Function (SPTMS)

The safety-related SPTMS is provided to monitor pool temperatures under all operating and accident conditions. The system operates continuously during reactor operation. Should the suppression pool temperature exceed established limits, the SPTMS provides input for both a reactor scram and for automatic initiation of suppression pool cooling mode of FAPCS. The SPTMS is part of the Containment Monitoring System (CMS).

7.1.1.4 Engineered Safety Features Systems

Emergency Core Cooling Systems (ECCS)

Safety-related I&C provides automatic initiation and control of the Isolation condensers, Automatic Depressurization System (ADS) and the Gravity-Driven Cooling System (GDCS) to cool the fuel cladding in event of a design basis accident. The Standby Liquid Control (SLC) System also has an ECCS function discussed in Section 7.4.

Isolation Condenser System (ICS)

Safety-related ICS I&C automatically limit reactor pressure and temperature within an acceptable range so that safety relief valves will not lift and emergency reactor depressurization action will not occur when the reactor becomes isolated during power operations. Over longer durations, the ICS also removes excess sensible and core decay heat from the reactor without the need for an external power supply, and with minimal loss of coolant inventory from the reactor when the normal heat removal system is unavailable.

Passive Containment Cooling System (PCCS)

The safety-related PCCS functions to cool the containment following a rise in containment pressure and temperature without requiring any component actuation.

The PCCS needs no electric power and does not have instrumentation, control logic, or power actuated valves. Therefore, PCCS is not addressed in Chapter 7. However, the PCCS is briefly described herein for completeness.

Leak Detection and Isolation System (LD&IS)

The safety-related LD&IS I&C monitors leakage sources from the reactor coolant pressure boundary, and automatically initiates closure of the appropriate isolation valves to isolate the

source of the leak if monitored system variables exceed preset limits. This action limits the loss of coolant from the reactor coolant pressure boundary and the release of radioactive materials to the environment.

Safety System Logic and Control System (SSLC)

The safety-related SSLC includes the control functions of the various safety function actuation devices of the safety-related plant systems. Input signals from redundant channels of safety-related instrumentation are used to perform logic operations that result in decisions for safety action. Trip logic outputs to the actuation devices (pilot solenoid valves, squib valves, etc.) initiate the appropriate plant protection.

7.1.1.5 Safety and Non-Safety Shutdown Systems

Standby Liquid Control (SLC) System

The safety-related SLC system I&C provides for the automatic initiation of an independent boron solution system, to shut down the reactor from rated power to shutdown conditions in the event that withdrawn control rods cannot be inserted to achieve reactor shutdown. The system is also automatically initiated with ADS to provide additional core inventory.

Remote Shutdown System (RSS)

Should the main control room become uninhabitable, the RSS panel provides the ability to both monitor and operate all of the required systems within the corresponding division. Although no automatic functions are lost with the control room evacuation, manual operation of all the divisional systems is also available. Similarly each RSS panel includes the ability to operate all of the non-safety Plant Investment Protection (PIP) equipment and BOP equipment, either automatically or manually.

Reactor Water Cleanup/Shutdown Cooling System (RWCU/SDC)

Nonsafety-related RWCU/SDC I&C functions to maintain reactor water purity during operation, and to provide normal shutdown cooling by taking suction from the reactor pressure vessel, pumping the flow through heat exchangers, and returning the cooled water to the vessel through the feedwater line. The I&C system is segmented and allows the different “A/B” components to operate independently.

Fuel and Auxiliary Pools Cooling System (FAPCS)

Nonsafety-related FAPCS I&C functions to maintain the various ICS, GDCS and suppression pool temperatures and cleanliness during operation, by pumping the flow through heat exchangers and demineralizers. The FAPCS can also provide a “Low Pressure Core Injection (LPCI)” mode to provide inventory after the reactor pressure has been reduced. The I&C is segmented and allows the different “A/B” components to operate independently.

Control Rod Drive System (CRD)

Nonsafety-related CRD I&C normally functions to maintain the HCU accumulators at the required pressure, to provide cooling water flow to the FMCRDs and to provide various high pressure purge flows. The CRD can also provide a “high pressure injection” mode capable of supplying inventory to the reactor vessel at elevated pressures. The I&C is segmented and allows the different “A/B” components to operate independently.

7.1.1.6 Safety-Related Information Systems

General I&C Conformance to Regulatory Guide 1.97

Safety-related display instrumentation provides information regarding plant conditions and equipment status in order to determine the need for manual safety action. A detailed assessment of ESBWR conformance with Regulatory Guide 1.97 is presented in Subsection 7.5.1.

Containment Monitoring System (CMS)

Safety-related CMS instrumentation measures and records radiation levels and the oxygen/hydrogen concentration levels in the primary containment under post-accident conditions. It is designed to operate continuously in normal operation and is automatically put in service upon detection of loss-of-coolant accident (LOCA) conditions.

Process Radiation Monitoring System (PRMS)

Safety-related and nonsafety-related PRMS instrumentation monitors the main steam lines, fission products in the drywell, discharges from the Isolation Condenser System, vent discharges and liquid and gaseous effluent streams that may contain radioactive materials. Main control room display, recording, and alarm capability are provided along with controls, which provide automatic trip inputs to the respective systems for isolation of further radiation release.

Area Radiation Monitoring System (ARMS)

Nonsafety-related ARMS instrumentation continuously monitors the gamma radiation levels within designated areas of the plant, and provides early warning to operating personnel when predetermined exposure rates are exceeded.

7.1.1.7 Interlock Systems

Systems Interlock Function

A reactor pressure interlock is provided to Gravity-Driven Cooling System (GDCS) to prohibit inadvertent manual initiation of the system during normal reactor operation.

Normally closed isolation valves are provided on the Fuel and Auxiliary Pools Cooling System (FAPCS) low-pressure injection (LPCI) line to protect its low pressure piping from over pressurization during the reactor power operation. A high pressure/low pressure interlock is provided to prevent opening of the isolation valve when the reactor pressure is higher than the FAPCS design pressure.

Interlock Systems

Redundant reactor pressure instruments provide a high-pressure signal to FAPCS HP/LP interlock when the reactor pressure exceeds the setpoint determined based on the design pressure of the low pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock circuit initiates a signal to close the isolation valves and prevent them from opening.

Other than the isolation valves, the ESBWR design has no interlocks that isolate safety-related from nonsafety-related piping during LOCA, because there are no piping interfaces separating safety-related and nonsafety-related portions of piping systems.

7.1.1.8 Control Systems

Nuclear Boiler System Instrumentation

Redundant safety-related instrumentation is provided to monitor reactor vessel water level and reactor vessel pressure for operator monitoring and inputs to safety systems during normal, transient, and accident conditions.

Nonsafety-related instrumentation provides indication of reactor coolant and vessel temperatures, reactor vessel water level, and reactor vessel pressure.

Rod Control and Information System

Nonsafety-related I&C provide the capability to control reactor power level by controlling the movement of the control rods in the reactor core during manual, semi-automated, and automated modes of plant operations. The automated thermal limit monitor (ATLM) subsystem automatically enforces fuel operating thermal limits minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) when reactor power is above the low power setpoint (LPSP).

Feedwater Control System (FWCS)

A highly reliable and triplicate redundant nonsafety-related I&C both automatically and manually regulates the flow of feedwater into the reactor pressure vessel to maintain predetermined water level limits during minor transients and normal plant operating modes.

Plant Automation System (PAS)

Nonsafety-related I&C provides automatic startup/shutdown algorithms and controls, regulates reactivity during criticality control, provides heatup & pressurization control, regulates reactor power, and provides automatic power generation control during power operation.

Steam Bypass and Pressure Control System (SBPC)

A highly reliable and triplicate redundant nonsafety-related I&C controls reactor pressure during plant startup, power generation and shutdown modes of operation, by directly controlling the turbine bypass and indirectly controlling turbine control valve position by sending pressure regulation demand signals to the Turbine Control System - Electro-Hydraulic Control.

Neutron Monitoring System - Nonsafety-related Subsystems

The nonsafety-related Automated Fixed In-core Probe (AFIP) provides a signal proportional to the axial neutron flux distribution at the radial core locations of the Local Power Range Monitor (LPRM) detectors. The signal facilitates fully automated, precise, reliable calibration of LPRM gains and provides axial power measurement data for three dimensional core power distribution determination. The nonsafety-related MRBM Subsystem logic issues a rod block signal that is used in the RCIS logic to enforce rod blocks that prevent fuel damage by assuring that the minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) do not violate fuel thermal safety limits.

Containment Inerting System

Nonsafety-related I&C establishes and maintains an inert atmosphere within the primary containment during plant operating modes, except during plant shutdown for refueling or

equipment maintenance and during limited periods of time to permit access for inspection at low reactor power.

7.1.1.9 Diverse Instrumentation and Controls

Although not required for safety, Diverse I&C is provided to address Branch Technical Position HICB-19 on Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems, in addition to the ATWS mitigation features, which provide alternate control rod insertion, boron injection, and feedwater runback. (The ATWS mitigation function using liquid boron injection is part of diverse I&C functions, which is safety-related and is included as part of SSLC.) This diverse I&C function, called Diverse Protection System (DPS), is implemented in a highly reliable triplicate redundant control system whose sensors, hardware and software are different than any of the safety-related I&C platforms.

The following diverse actuation functions are provided in this DPS:

(1) A set of protection logics that provide diverse means to scram the reactor via control rod insertion using separate and independent sensors, hardware and software from the primary RPS.

(2) A set of ESF initiation logics that provide diverse means to initiate certain ESF functions using separate and independent sensors, hardware and software from the primary ESF systems.

(3) A set of alternate rod insertion (ARI) and associated logics (e.g., control rod run in) via control rod insertion through alternate means by opening the three sets of air header dump valves of the Control Rod Drive system. This is also part of the ATWS mitigation function.

The diverse protection system provides both manual and automatic initiation of the above functions.

7.1.1.10 Data Communication Systems

The Essential Distributed Control & Information System (E-DCIS) and Non-Essential Distributed Control & Information System (NE-DCIS) provide distributed control and instrumentation data communications networks to support the monitoring and control of interfacing plant safety and non-safety systems. They provide the electrical devices and circuitry (such as multiplexing units, data transmission line and transmission controllers) between sensors, display devices, controllers and actuators. They also provide acquisition and communication software required to support the function of transmitting plant-wide data for distribution control and monitoring.

Within the NE-DCIS, the various distributed plant computers and workstations support both display, alarm, monitoring and control functions that increase the efficiency of plant performance by performing functions, calculations and nonsafety-related system controls during startup, normal, and shutdown modes of plant operation. The various plant computers additionally provide both local and permanently archived records of plant operation. The plant computer functions also drive nonsafety-related display and control equipment in the main control room and provide supervisory control of plant automation features.

7.1.2 Identification of Design Bases and Safety Criteria

7.1.2.1 General

The I&C design bases address the performance of the systems intended function while satisfying the applicable general design criteria, regulatory guides, industry standards, and other documents.

The safety design basis for a safety-related system states the unique functional design requirements that establish the limits to satisfy the safety objectives. The general functional requirement portion of the safety design basis presents those requirements that have been determined to be sufficient to ensure the adequacy and reliability of the system from a safety viewpoint.

10 CFR 50.2 Safety Design Bases

Safety-related systems provide actions necessary to assure safe plant shutdown to protect the integrity of radioactive material barriers or prevent the release of radioactive material in excess of allowable dose limits for design basis accidents. These safety-related systems consist of components, groups of components, systems, or groups of systems. A safety-related system may have a power generation design basis. The unique functional design requirements stated in the design basis establish the limits to satisfy the safety objectives

The technical design bases for the instrumentation and controls for each system are presented as specific subsections throughout Chapter 7.

Nonsafety Design Bases

Nonsafety-related (including power generation) systems are reactor support systems that are not required to protect the integrity of radioactive material barriers and do not prevent the release of radioactive material in excess of allowable dose limits. The I&C portions of these system may prevent the plant from exceeding preset limits that would otherwise initiate the action of safety-related systems.

Instrument Errors

The design considers instrument drift, environmental conditions at the sensor location, changes in the process, testability, and repeatability in the selection of instrumentation and controls and in the determination of setpoints. Adequate margin between safety limits and instrument setpoints is provided to allow for instrument error. The safety limits and allowable values are provided in the plant Technical Specifications. The amount of instrument error is determined by test and experience. The setpoint is selected based on the known error; since almost all of the I&C is microprocessor based and almost all of the instrument loop error is in the sensor since discrete setpoints do not drift. The recommended test frequency is greater on instrumentation that demonstrates a stronger tendency to drift.

The system allowable values for setpoints are listed in the plant Technical Specifications for each safety-related system. The actual settings are determined based on operating experience and conservative analyses. The settings are high enough to preclude inadvertent initiation of the safety action but low enough to assure that significant margin is maintained between the actual setting and the limiting safety-related system settings. The margin between the limiting safety-

related system settings and the actual safety limits includes consideration of the maximum credible transient in the process being measured.

The periodic test frequency for each variable is determined from historical data on setpoint drift and from quantitative reliability requirements for each system and its components. . More detailed information on consideration of instrument error and on setpoint calculation is included in Reference 7.2-1, "General Electric Instrument Setpoint Methodology."

Testing and Inspection

The testing and inspection capabilities for the instrumentation and controls for each system are presented as specific subsections in Chapter 7.

7.1.2.2 Conformance to Regulatory Requirements and Industry Standards

The applicability of the following regulatory requirements and industry standards to the instrumentation and controls for the various systems are presented in the following subsections:

- Title 10 Code of Federal Regulations, including TMI Action Plan Requirements
- NRC Regulatory Guides
- Industry codes and standards
- Branch Technical Positions

The specific regulatory acceptance criteria and guidelines requirements applicable to each of these systems (safety-related or nonsafety-related but important for plant operation) identified in the Standard Review Plan are identified and tabulated in Table 7.1-1. The regulatory requirements applicability matrix of Table 7.1-1 is followed in Section 7.2 through Section 7.9 for the regulatory conformance discussions of each specific system. The degree of applicability and conformance, along with any clarifications or justification for exceptions, are presented in the evaluation sections for each specific system. General I&C conformance is discussed in the following subsections. For those safety I&C systems that are identical or very similar in architecture design to those previously reviewed by NRC (ABWR Certification), or those where the adequacy of the system is based upon prior NRC approval, such architecture design of those systems are identified in the system description sections of each specific system.

Title 10 Code of Federal Regulations

10 CFR 50.55a (Codes and Standards):

10 CFR 50.55a(a)(1) and 50.55a(h) are applicable to the instrumentation and control equipment. 10 CFR 50.55a(h) requires the application of IEEE 279 for protection systems. However, Regulatory Guide 1.153, Section B, states: "Compliance with the provisions of IEEE Std. 603-1980, as supplemented in Section C of this guide, is considered by the NRC staff to satisfy the provisions of IEEE Std. 279-1971." Therefore, because RG 1.153 (IEEE 603) is addressed for each system, IEEE 279 is not separately addressed.

10 CFR 50.34(f) (Conformance to TMI Action Plan Requirements):

Response to TMI related matters is generally addressed in Chapter 1, Appendix 1A. TMI action plan requirements are identified relative to the C&I systems in Table 7.1-1. The applicable

systems are generally designed to conform. However, because of the design features of the ESBWR, several of these requirements are not applicable. These are identified as follows:

II.K.3.13 - HPCI and RCIC Initiation Levels

II.K.3.15 - Isolation of HPCI and RCIC (Turbine Driven)

II.K.3.21 - Automatic Restart of LPCS and LPCI

II.K.3.22 - RCIC Automatic Switchover of Suction Supply

For the others, the degree of conformance, along with any clarifications or exceptions, is discussed in the safety evaluation subsections of Sections 7.2 through 7.9.

10 CFR 50.62 (ATWS):

The ESBWR is designed with ATWS mitigation functions, as described in Section 7.8.

10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii) Interface Requirements

- Conformance: Interface material is provided in Tier 1.

10 CFR 52.47(a)(2) Level of Detail

- Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this BTP.

10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

- Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

10 CFR 52.79(c), ITAAC in Combined License Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 50 Appendix A, General Design Criteria (GDC):

Conformance with NRC General Design Criteria (10 CFR 50 Appendix A) is discussed in Section 3.1. The applicability of GDC to each system is presented in Table 7.1-1. Specific conformance of the I&C systems themselves is addressed in Sections 7.2 through 7.7.

Staff Requirements Memoranda (SRM)

SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures):

The ESBWR digital I&C is designed with defense-in-depth and diversity for defense against common-mode failures. Section 7.8 includes the description of the diverse instrumentation and control system that specifically addresses the requirements of this SRM.

SRM to SECY 93-087 II.T (Control Room Annunciator/Alarm Reliability)

Section II.T of SECY 93-087 applies specifically to the post-accident monitoring requirement, which is described in Section 7.5. The ESBWR alarm system meets the intent of the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant. Alarm points are sent via dual network to redundant message processors on dual power supplies. The processors are dedicated and only do alarm processing. The alarms are displayed on multiple independent VDUs (dual power supplies on each). The alarm tiles are driven by redundant data links (dual power). The alarm tile processor is redundant. Each alarm tile has at least two LEDs. The horn and voice speaker are not redundant. Test buttons are available to test the horn(s) and all the lights. There are no alarms requiring manually controlled actions for safety systems to accomplish their safety function. Thus the requirements for Class 1E equipment and circuits are not applicable.

Conformance to Regulatory Guides

A discussion of the general conformance of the I&C equipment to the Regulatory Guides is as follows. Individual system conformance, along with any clarifications or exceptions, is addressed in the Safety Evaluation subsections within Sections 7.2 through 7.9.

Regulatory Guide 1.22 - Periodic Testing of Protection System Actuation Functions - Safety-related systems have provision for periodic testing. Proper functioning of analog sensors can be verified by channel cross-comparison and is done continuously by the plant computer functions. Some actuators and digital sensors, because of their locations, cannot be fully tested during actual reactor operation. Such equipment is identified and provisions for meeting the requirements of Paragraph D.4 (per BTP HICB-8) are discussed in the Safety Evaluation subsections within Sections 7.2 through 7.9.

Regulatory Guide 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - Bypass indications are designed to satisfy the requirement of IEEE 603, Paragraph 5.8.3, and Regulatory Guide 1.47. The design of the bypass indications allows testing during normal operation and is used to supplement administrative procedures by providing indications of safety-related systems status.

Bypass indications are designed using isolation devices that preclude the possibility of any adverse electrical effect of the bypass indication circuits on the plant safety-related system.

Regulatory Guide 1.53 - Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems - The safety-related system designs conform to the single failure criterion.

Regulatory Guide 1.62 - Manual Initiation of Protective Actions - Manual initiation of the protective action is provided at the system level for safety-related systems.

Regulatory Guide 1.75 - Physical Independence of Electric Systems - The safety-related system designs conform to the physical independence criterion.

The I&C of the safety-related systems complies with the independence and separation criteria for redundant systems in accordance with Regulatory Guide 1.75 or by implementation of the following alternates:

- Associated circuits installed in accordance with IEEE 384, Subsection 5.5.2(1), are subject to the requirements of Class 1E circuits for cable derating, environmental

qualification, flame retardants, splicing restrictions, and raceway fill unless it is demonstrated that Class 1E circuits are not degraded below an acceptable level by the absence of such requirements.

- The method of identification used (IEEE 384, Subsection 6.1.2) preclude the need to frequently consult any reference material to distinguish between Class 1E and non-Class 1E circuits, between non-Class 1E circuits associated with different redundant Class 1E systems, and between redundant Class 1E systems.
- First sentence of IEEE 384, Section 6.8 is implemented as follows:
  - Redundant Class 1E sensors and their connections to the process system shall be sufficiently separated so that required functional capability of the protection system are maintained despite any single design basis event.
- Non-Class 1E instrumentation circuits are exempted from the provisions of IEEE 384, Section 5.6, provided they are not routed in the same raceway as power and control cables (unless the cables are optical fiber) or are not routed with associated cables of a redundant division.

Regulatory Guide 1.97 - Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant Conditions During and Following an Accident - Instrumentation and controls are designed to meet the requirements of Regulatory Guide 1.97. Details of design implementation are discussed in Section 7.5.

Regulatory Guide 1.105 - Instrument Setpoints for Safety-Related Systems - The instrumentation and control systems are consistent with the requirements of Regulatory Guide 1.105. The applicable trip setpoint (instrument setpoint) allowance value (technical specification limit) and the analytical or design basis limit are provided in separate documentation. These parameters are appropriately separated from each other based on instrument accuracy, calibration capability and design drift (estimated) allowance data. The setpoints are within the instrument best-accuracy range. The established setpoints provide margin to satisfy both safety requirements and plant availability objectives.

Regulatory Guide 1.118 - Periodic Testing of Electric Power and Protection Systems - The instrumentation and control systems are consistent with the requirements of Regulatory Guide 1.118, with the following clarifications of the regulatory guide requirements:

- Position C.6b - Trip of an associated protective channel or actuation of an associated Class 1E load group is required on removal of fuses or opening of a breaker only for the purpose of deactivating instrumentation or control circuits.
- Position C.2 - Insofar as is practical and safe, response time testing is performed from sensor inputs (at the sensor input connection for process instruments) to and including the actuated equipment.

Regulatory Guide 1.151 Instrument Sensing Lines - The instrument sensing lines are designed to satisfy the requirements of Regulatory Guide 1.151. Such lines are used to perform both safety-related and nonsafety-related functions. However, there are four redundant and separate sets of instrument lines, each having Class 1E instruments associated with one of the four electrical Class 1E divisions. The Reactor Protection System logic requires any two out of the

four signals to scram. If a channel is bypassed, the logic is two-out-of-three. Also, emergency core cooling functions are redundant throughout the four divisions and the feedwater system is designed with fault-tolerant triplicate digital controllers using separate sensors from the safety-related sensors. Therefore, the systems are designed such that no single failure could cause an event and at the same time prevent mitigating action for the event.

Regulatory Guide 1.152 - Computer Software Used in Safety-Related Systems - Criteria and guidelines stated in ANSI/IEEE-ANS-7-4.3.2, as endorsed by Regulatory Guide 1.152 are used as a basis for design procedures established for programmable digital equipment.

DG-1130/IEEE Std. 7-4.3.2-2003 Summary

Regulatory Guide 1.152 is the main regulatory guide on digital computers in safety systems in nuclear power plant. Draft Regulatory Guide DG-1130 will become RG 1.152 Rev.2 after it is officially issued. DG-1130 endorses and refers to IEEE 7-4.3.2 – 2003 and IEEE 603-1998 for specific criteria details.

The content of DG-1130 is similar to Regulatory Guide 1.152 Rev.1, except in certain areas that some additional requirements are specified. One major requirement area in DG-1130 contains discussions on digital I&C equipment common mode failure issues. The concern is related to the possibility that a design error in the software in redundant channels of a safety system could lead to common-cause or common-mode failure of the safety system function. Conditions may exist under which some form of diversity may be necessary to provide additional assurance beyond that provided by the design and QA programs that incorporate software QA and V&V. The design techniques of functional diversity, design diversity, diversity in operation, and diversity within the four echelons of defense in depth can be applied as defense against common-cause failures. The justification for equipment diversity, or for the diversity of related system software such as a real-time operation system, must extend to equipment components to ensure that actual diversity exists. Claims for diversity based on different manufacturers are insufficient without consideration of the above. Other considerations such as functional and signal diversity, that lead to different software requirements form a stronger basis for diversity. DG-1130 endorses IEEE Std. 7-4.3.2 – 2003. It also refers to NUREG SRP Sec 7 BTP HICB-19 (June 1997 Rev.4) for additional guidance. DG-1130 contains extensive requirements on “Security.”

The following positions are noted in IEEE Std. 7-4.3.2-2003:

- The main text portions of IEEE 7-4.3.2 is similar to its 1993 version, with more extensive requirements incorporated, i.e., software development, V&V, software configuration management, equipment qualification, self-diagnostics, independence, reliability. There is no specifics details on diverse method requirements.
- Annex B "Diversity Requirements Determination“ basically the same as the 1993 version. This annex provides a methodology for determining the need for diversity. Three approaches are mentioned: functional diversity (e.g., ATWS); defense-in-depth analysis (design features diversity analysis in different echelons such as RPS, ESF, controls, etc); diverse design (combination of computer and non computer channels, separate specs/hardware/software, etc.) This annex requirements are "soft" such that in both of the first two approaches it stated that it is acceptable to use identical software. NRC DG-1130 does not endorse this Annex B.

- Annex C "Dedication of existing commercial computers": This is similar to the 1993 version. NRC does not endorse this annex.
- Annex E, "Communication Independence": This is similar to the annex in the 1993 version. NRC does not endorse this annex.
- Annex F, "Computer reliability": This is similar to the annex in 1993 version. NRC states that quantitative reliability goals are not the only means, and does not endorse this method as the sole means of meeting the regulations for reliability of digital computers. NRC acceptance is based on deterministic criteria.

ESBWR Safety I&C System compliance to DG-1130/IEEE Std. 7-4.3.2-2003

Regulatory Guide 1.152 Rev.1 has been followed in the design of ABWR safety I&C systems, and the ESBWR safety I&C, being very similar or identical in design approach and in safety design requirements, also meets the requirements of Regulatory Guide 1.152 Rev.1. DG-1130 includes additional requirements applicable to digital computer-based safety I&C equipment. The ESBWR compliance to these additional DG-1130 requirements are summarized as follows.

Defense against software common mode failures: GE has evaluated BTP-HICB-19 requirements including the acceptance criteria on defense-in-depth and diversity and defense against common mode failures, on the four echelons of defense against common-mode failures: control systems, reactor trip system, ESFAS, and monitoring and indicators functions. Based on GE's evaluation, to fully address the requirements of BTP HICB-19 and DG-1130 on defense-in-depth and diversity and defense against common mode failures, the Diverse Protection System (DPS) is developed to back up the primary safety I&C system protection functions. The DPS is implemented with totally separate and independent equipment from the primary Safety I&C protection systems (RPS and SSLC/ESF). The DPS is implemented in addition to the ATWS/Standby Liquid Control System function.. Detailed description of the DPS and the description of defense-in-depth and diversity and defense against common mode failure are included in Section 7.8

Based on GE's evaluation, to fully meet the requirements of DG-1130 and BTP HICB-19 following the principle of defense-in-depth and diversity and protection against software common mode failures, the ESBWR safety protection systems (RPS and SSLC/ESF Initiation Logics) are backed up by a totally separated and independent Diverse Protection System in which key protection functions of the RPS and SSLC/ESF are duplicated using totally separate sensor inputs and separate equipment. This Diverse Protection System is implemented in addition to the ATWS/Standby Liquid Control System using liquid boron injection to shutdown the plant. This Diverse Protection system is a nonsafety system with redundant channels but with software language diverse from the RPS and SSLC/ESF. The Diverse Protection System satisfies the requirements specified in BTP HICB-19 and DG-1130. Detailed description of the Diverse Protection System and discussion of defense against common mode failures are included in Section 7.8.

Software development process: The software development process of the ESBWR safety I&C systems (including control systems important for plant operation) will follow the guidelines of BTP HICB-14. Software development process plans will be developed for ESBWR safety I&C design implementation including Software Management Plan, Software Development Plan, Software Verification and Validation Plan, Software Configuration Management plan, and

Software Safety Plan, etc., as required by BTP HICB-14. Actual detailed hardware and software design implementation will follow the guidelines specified by these plans as part of the DAC process.

Equipment qualification, self-diagnostics, independence, reliability: IEEE Std. 603 specifies these requirements applicable to safety I&C system equipment, as described in Subsection 7.1.2.3.3. The ESBWR safety I&C systems meet the requirements of IEEE Std. 603, and above requirements in areas applicable to digital computer-based equipment.

Security: The security requirements included in DG-1130 will be evaluated and incorporated as appropriate and needed in the ESBWR safety I&C design, both on plant hardware security measures and software security measures. The software development process plans will be developed with the security requirements incorporated for actual detailed design implementation.

Regulatory Guide 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems - Safety-related systems are designed to satisfy the requirements of IEEE 603, as endorsed by Regulatory Guide 1.153. Clarifications or exceptions (if any) for any of the provisions are discussed in the individual systems safety evaluation sections.

Regulatory Guide 1.168 - Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants.

This regulatory guide endorses IEEE Std. 1012, IEEE Standard for Software Verification and Validation Plans, and IEEE Std. 1028, IEEE Standard for Software Reviews and Audits. IEEE Std. 1012 is acceptable for providing high functional reliability and design quality in software used in safety systems. IEEE Std. 1028 is acceptable for carrying out software reviews, inspections, walkthroughs, and audits subject to certain provisions. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.169 - Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 828, IEEE Standard for Software Configuration Management Plans, and ANSI/IEEE Std. 1042, IEEE Guide to Software Configuration Management. These standards, with the clarifications provided in the Regulatory Position, describe acceptable methods for providing high functional reliability and design quality in software used in safety systems. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.170 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

The requirement contained in IEEE Std. 829, IEEE Standard for Software Test Documentation, provide an acceptable approach for meeting the requirements of 10 CFR Part 50 as they apply to the test documentation of safety system software subject to the provisions in this guide. Safety-related systems such as SSLC software development uses the guidance in these standards as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.171 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 1008, IEEE Standard for Software Unit Testing, subject to the provisions in this guide. This standard defines an acceptable method for planning, preparing for, conducting, and evaluating software unit testing. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 830, Recommended Practice for Software Requirements Specifications, as amended in the Regulatory Position. This standard describes current practice for writing software requirements specifications for a wide variety of systems. It is not specifically aimed at safety applications; however, it does provide guidance on the development of software requirements specifications that will exhibit characteristics important for developing safety system software. This is consistent with the goal of ensuring high-integrity software in reactor safety systems. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Regulatory Guide 1.173 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants

This regulatory guide endorses IEEE Std. 1074. The standard describes, in terms of inputs, development, verification or control processes, and outputs, a set of processes and constituent activities that are commonly accepted as composing a controlled and well-coordinated software-development process. It describes inter-relationships among activities by defining the source activities that produce the inputs and the destination activities that receive the outputs. The standard specifies activities that must be performed and their inter-relationships; it does not specify complete acceptance criteria for determining whether the activities themselves are properly designed. Therefore, the standard should be used in conjunction with guidance from other appropriate regulatory guides, standards, and software engineering literature. Safety-related systems such as SSLC software development uses the guidance in this standard as discussed in Appendix 7B to develop portions of the overall software development plan and thus complies with this regulatory guide.

Conformance to Industry Standards

The safety evaluation subsections throughout Chapter 7 address the regulatory guides in accordance with the SRP. Those IEEE standards that are endorsed by regulatory guides are not addressed separately.

Other codes or standards not mentioned in the SRP may be utilized in specific system applications. These are identified in the system description and the corresponding reference section. Some IEEE standards applicable to the I&C equipment are addressed in other chapters in accordance with the SRP format. These are identified as follows:

IEEE 323 - Qualifying Class 1E Equipment for Nuclear Power Generating Stations - Safety-related systems are designed to meet the requirements of IEEE 323. Environmental qualification is addressed in Section 3.11.

IEEE 344 - Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations - Safety-related instrumentation and control equipment is classified as Seismic Category I and designed to withstand the effects of the safe shutdown earthquake (SSE) and remain functional during normal and accident conditions. Qualification and documentation procedures used for Seismic Category I equipment and systems satisfy the provisions of IEEE 344 as indicated in Section 3.10.

Conformance to Branch Technical Positions

Applicable branch technical positions (BTPs) are identified relative to the C&I systems in Table 7.1-1. The systems are generally designed to conform to the BTPs. The degree of conformance, along with any clarifications or exceptions, is discussed in the Safety Evaluation subsections of Sections 7.2 through 7.9.

In the BTP HICB-16 requirements, it is stated that the application should (1) describe the resolution of unresolved and generic safety issues applicable to the I&C systems, and (2) describe the interface requirements to be met by portions of the plant for which the application does not seek certification and which are necessary to ensure proper functioning of the I&C system, and (3) identify and describe the validation of innovative means of accomplishing I&C system safety functions. Applications that propose the use of computers for systems important to safety should describe the computer system development process. Applications that propose the use of computers for reactor trip system (RTS) and engineered safety features actuation system (ESFAS) functions should also describe the design of the overall I&C systems with respect to defense-in-depth and diversity requirements.

The ESBWR does not have any unresolved and generic safety issues applicable to the I&C systems. Such unresolved and generic safety issues are described in DCD Section 1.11. There are several new generic issues that are related to I&C systems, such as failure of protective devices on essential equipment, Electromagnetic pulse, identification of protection system instrument sensing lines, and protection system testability. The above issues either are not applicable to ESBWR safety I&C systems design or the ESBWR has addressed those issues in its safety I&C design.

Within the scope of the ESBWR DCD submitted for certification application, there are no such interface requirements as described here that falls into the above category.

The validation of innovative means of accomplishing I&C system safety-related functions does not apply to the ESBWR safety I&C design submitted for this certification application.

For the description of computer system development process, the compliance to BTP HICB-14 is explained and summarized in Appendix 7B of this chapter. GE will prepare and submit to NRC the software development process plans required by BTP HICB-14 for NRC's review and approval, as part of the ESBWR Certification activity.

ESBWR safety I&C systems (RPS and SSLC/ESF) use computers for their logic functions. Description of the safety I&C systems design with respect to defense-in-depth and diversity and defense against common mode failures is included in Section 7.8, together with the description

of the Diverse Protection system, which specifically addresses to the issues of defense-in-depth and diversity and defense against common mode failures.

7.1.2.3 Conformance to 10 CFR 50.55a(h) and IEEE Std. 603

As requested by 10 CFR 50.55a(h), IEEE Std. 603 endorsed by Reg. Guide 1.153, superceding IEEE Std. 279, is followed for compliance of criteria for safety systems for nuclear power generation stations. In this section, a summary description is included to demonstrate the overall ESBWR safety I&C systems compliance of IEEE Std. 603, according to the guidelines described in NUREG 0800, SRP Appendix 7.1-C. For specific descriptions of functional compliances of the IEEE Std 603 criteria by various safety-related systems, the discussions are referred to the various subsections of this chapter, as listed in the various sections below.

7.1.2.3.1 Scope per IEEE Std. 603

The scope of IEEE Std 603 includes all I&C safety systems which are systems covered in Section 7.2 through 7.6. Except for the requirements for independence between control systems and protection systems, IEEE Std 603 does not directly apply to nonsafety systems. Applicable considerations include design basis, redundancy, independence, single failures, qualification, bypasses, status indication, and testing. The IEEE Std 603 also applies to those parts of the digital data communication that supports safety system functions. The design of ESBWR I&C safety systems is in compliance with the IEEE Std 603 requirements as described in the above scope, based on the definition and explanation of IEEE Std 603 Section 1.

7.1.2.3.2 Safety System Designation (Design Basis) per IEEE Std. 603

Section 4 of IEEE Std 603 requires in part that a specific basis be established for the design of each safety system. The design basis should address all system functions necessary to fulfill the system's safety intent. The design basis should address the requirements of 10 CFR 50 Appendix A, GDC 20, which requires that the protection system be initiated automatically to assure that acceptable fuel limits are not exceeded, and that accident condition be sensed so to initiate the operation of systems and components important to safe plant operation. This GDC mainly addresses to reactor trip systems (RTS) and engineered safety features actuation systems (ESFAS). Information provided for each design basis item should be sufficient to enable the detailed design of the system to be carried out. The design of ESBWR I&C safety systems is in compliance with the IEEE Std 603 requirements as described in the above summary. Safety system design basis descriptions are included in the various sections of this chapter as indicated below.

Reactor Trip System:

- Reactor Protection System: Subsection 7.2.1.1
- Neutron Monitoring System: Subsection 7.2.2.1

Suppression Pool Temperature Monitoring: Subsection 7.2.3.1

Engineered Safety Features Systems:

- Emergency Core Cooling System: Subsection 7.3.1
- Leak Detection and Isolation System: Subsection 7.3.3.1

Safety System Logic and Control: Subsection 7.3.4.1

Standby Liquid Control System: Subsection 7.4.1.1

Remote Shutdown System: Subsection 7.4.2.1

Reactor Water Cleanup/Shutdown Cooling System: Subsection 7.4.3.1

Isolation Condenser System: Subsection 7.4.4.1

Containment Monitoring System: Subsection 7.5.2.1

7.1.2.3.3 Safety System Criteria per IEEE Std. 603

This section mainly requires that the safety systems shall maintain plant parameters within acceptable limits established by design basis events, that the safety systems meet all key design criteria stated in this section, and that the protection system has been qualified to demonstrate that the performance requirements are met.

Single Failure Criterion (IEEE-603, 5.1)

This section requires that any single failure within the safety system shall not prevent proper protective action at the system level when required, and it should be confirmed that requirements of the single failure criterion are satisfied. The ESBWR safety-related I&C systems satisfy the single failure criteria. All safety-related I&C systems have multiple (four) redundant and independent channels, including redundant and independent sensors assigned to each of the redundant channels. The trip logic is 2-out-of-4 logic. Any failed channel caused by single failure associated with this channel does not affect the safety system to perform its safety protection functions because of this 2-out-of-4 logic. The failed channel can be bypassed without affecting the performance of the safety system functions, with the logic reverted to 2-out-of-3. Descriptions of design of the safety-related I&C systems that addressed the single failure criterion are included in the various subsections as shown in Table 7.1-2.

Digital computer-based I&C systems share data, data transmission, and functions which may become a source of concern that a design using shared databases and process equipment has the potential to propagate a common-mode failure of redundant equipment. The ESBWR safety-related I&C systems include a diverse protection system design to specifically address and mitigate any common-mode failure concern of digital computer-based systems. This design, in addition to the ATWS/SLC system design, fully addresses the requirements of Staff Requirements Memorandum SECY-93-087 and BTP HICB-19. This design is described in Section 7.8.

Completion of Protective Action (IEEE Std. 603, 5.2)

In the ESBWR, completion of protective action, once initiated automatically or manually, is accomplished by the RPS with seal in logic. Specific description is included in Subsection 7.2.1.2 and in other subsections as shown in Table 7.1-2.

Quality (IEEE Std. 603, 5.3)

All equipment is provided under GE's Appendix B quality program. The NRC accepted GE Quality Assurance Program with its implementing procedures constitute the Quality Assurance system that is applied to the GE ESBWR safety-related I&C system design. It satisfies all

applicable requirements of the following: 1) 10 CFR 50 Appendix B; 2) ANSI/ASME NQA-1; 3) ISO 9001. As an example, Section 9 of Reference 7.1-5 describes special quality program aspects related to GE's programmable digital safety-related I&C equipment.

Equipment Qualification (IEEE Std. 603, 5.4)

It is required that safety system equipment be designed to meet the functional performance requirements over the range of normal environmental conditions for the area in which it is located. Equipment qualification typically includes electromagnetic interference qualification, seismic qualification, and other environmental condition qualification such as temperature, humidity, radiation, and pressure. The ESBWR safety I&C systems are designed to meet the equipment qualification requirements set forth in IEEE Std. 603 and other associated equipment qualification requirements. The qualification was established using qualification methods set forth in General Electric Environmental Qualification Program, (Reference 7.1-7). The ESBWR safety I&C system components are designed to be qualified to operate in the normal and abnormal environments in which they are located.

For environmental qualification, the following areas are addressed:

Temperature and Humidity: The ESBWR safety I&C components are designed to be qualified using type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified temperature range and relative humidity range. The components will be qualified in accordance with Reg. Guide 1.89 (IEEE 323 - 1974) and IEEE 323 – 1983. All qualification will be based on type testing. Plant-specific action will be required to confirm that the maximum control room temperatures plus mounting panel temperature rise, allowing for heat load of the safety I&C equipment, does not exceed the temperature limit, and that control room humidity is maintained within limits.

Pressure: The ESBWR safety I&C components are designed to be qualified by analysis to perform to specification for any absolute pressure in the range specified. Plant-specific action will be required to confirm that the maximum control room pressure does not exceed the specified limits.

Radiation: The ESBWR safety I&C components are designed to be qualified by analysis to perform within specification limits over its service life under the specified radiation conditions. Plant-specific action will be required to confirm that the maximum radiation levels where the equipment is located do not exceed the allowed limits.

Seismic Qualification: The ESBWR safety I&C components are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated within the specified seismic limits, and when mounted in accordance with the specified mounting methods. The ESBWR safety I&C components are to be qualified in accordance with the requirements of Regulatory Guide 1.100 (IEEE 344 - 1975). Qualification is based on type testing. Plant-specific action or analysis will be required to confirm that the maximum seismic accelerations at the mounting locations of the equipment do not exceed the allowed limits.

EMI Qualification: The ESBWR safety I&C components, when mounted in accordance with the specified mounting methods, are designed to be qualified by type testing and analysis to demonstrate that the components will perform all specified functions correctly when operated

within the specified EMI limits. The ESBWR safety I&C equipment is designed to be not susceptible to electromagnetic disturbances from neighboring modules and does not cause electromagnetic disturbances to neighboring modules. The EMI qualification design follows the requirements specified in Mil-Std-462D, Mil Std. 461D, and IEC Standard 801, depending the specific requirement conditions. The ESBWR safety I&C equipment is to be qualified to perform within its specifications continuously while exposed to EMI environmental limits at the hardware mounting location. EPRI Report TR-102323 (Reference 7.1-8) is used for the envelope limits. The EMI susceptibility and emissions testing is performed by type testing using. In addition to the equipment design considerations, plant-specific actions are required to establish practices to control emission sources, maintain good grounding practices and maintain equipment and cable separation. Reference 7.1-5 has included more detailed descriptions of equipment qualification practices of GE's typical safety-related I&C equipment used in ABWR and is applicable to ESBWR.

System Integrity (IEEE Std. 603, 5.5)

The safety I&C systems are required to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. Other areas that are necessary to address as requirements include adequate system real-time performance for digital computer-based systems to ensure completion of protective action, evaluation of hardware integrity and software integrity (software safety analysis, as part of BTP HICB-14 requirements), fail in a safe state upon loss of energy or adverse environmental conditions, and the requirements for manual reset.

The ESBWR safety I&C systems meet the integrity requirements described in IEEE Std. 603. The ESBWR Reactor Trip System functions fail in the tripped state. The ESF logics fail to a state that the actuated component remains as-is. For the ESBWR RTIF functions, inoperable input instrument being detected will lead to channel trip. Hardware and software failures detected by self-diagnostics will cause trip actuation. Also, failure of hardware and software will not inhibit manual initiation of protective functions. More descriptions of system integrity design consideration are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Independence (IEEE Std. 603, 5.6)

The independence requirements address the independence between redundant portions of a safety system, between the safety systems and the effects of design basis events, and between the safety systems and other systems. Three aspects of independence are addressed in each case, i.e., physical independence, electrical independence, and communication independence. The ESBWR safety I&C systems meet these requirements. The ESBWR safety I&C systems have four redundant and independent channels, which are physically independent and separated, with independent electrical power source applied to each channel. There are no common switches shared by the four channels. The sensors used for each of the four channels are independent and physically separated from one another. Communication directly between the four channels are limited to the minimum such as channel trip signals and bypass status signals, and are through proper isolation devices such as using optic fibers.

For the independence between the safety systems and the effects of design basis events, these requirements are achieved basically through proper equipment qualification. Safety equipment is qualified for continued functional capability under the environment and location, in which the

equipment is located where design basis events conditions are considered. Safety systems are totally separated and independent from nonsafety systems. Communication from safety systems to nonsafety systems is carried out with proper signal isolation devices (e.g., fiber optic cables) and data path gateway. Communication from nonsafety systems to safety systems are strictly prohibited, with only one exception, i.e., the data transmission of LPRM calibration gain adjustment factors which are calculated in the nonsafety plant computer function of the Non-Essential DCIS, to the safety-related LPRM/APRM equipment using proper signal isolation. However, this data transmission can only be implemented and accepted by the safety equipment with operator acknowledgment. This data transmission does not interfere with RPS or SSLC/ESF protection functions. More descriptions of safety system independence design are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Capability for Testing and Calibration (IEEE Std. 603, 5.7)

The capability for testing and calibration of safety system equipment are required to be provided during power operation and required to duplicate the performance of the safety function as closely as practicable. It is permitted that tests can be performed in overlapping test segments in order to test one safety function. Also, the I&C design should allow for tripping or bypass of individual functions in each safety system channel. The ESBWR safety I&C systems meet the requirements as outlined in this IEEE 603 section. The safety functions of each safety channel can be tested on line with the tested channel bypassed from the 2-out-of-4 trip logic. The I&C equipment has built-in self-diagnostic functions to identify critical failures such as loss of power and data errors, etc. More descriptions of system testing and calibration are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Information Displays (IEEE Std. 603, 5.8)

Displays for manually controlled actions: Type A variables are those variables that provide the primary information required for the control room operators to take the specified manual actions for which no automatic control is provided and that are required for safety-related systems to accomplish their safety functions for design basis accident events. For ESBWR, there are no instruments in this application as Type A variables. More discussion on this subject is included in Subsection 7.5.1.

System Status Indication: The ESBWR safety and nonsafety I&C systems are provided with system status information that meet the requirements of IEEE 603. All pertinent system trip/logic status, parameter data values, equipment functional status and ESF actuator status are available to be displayed to the operator upon request. For safety systems, such information is available for each division/channel. Certain information important to plant operation and status monitoring are permanently displayed (on large wide display panels) in the main control room. Alarm (and annunciation) indications are also available in the main control room per system design requirements. Other than post accident safety display, the system status information is not safety-related.

Indication of Bypasses: For safety system protection functions, bypass status is continuously displayed to the operator. All bypass status information is available to be displayed per system design requirements. Certain bypass information is accompanied with alarm, when activated not as under normal operation conditions. More descriptions of system bypass and alarm conditions

are included in the system description subsections of the respective safety systems as outlined in Table 7.1-2.

Location of Display: The locations of all displays located in the main control room are either on the main control console or on the large wide display panels visible and accessible to the operator. The ESBWR man machine interface system design (human system interface) includes design requirements and specifications on the classification of locations of various displays in the main control room. More detailed description of requirements on location of displays are included in Chapter 18, and the associated references of Chapter 18.

Control of Access (IEEE Std. 603, 5.9)

There are several means to implement access control to plant I&C equipment especially safety-related systems. Administrative control is used to implement control of access such as only qualified plant personnel is allowed to have access of keys (doors, cabinets, keylock switches) and passwords to get access to plant equipment especially safety systems equipment. Only qualified plant personnel is allowed to exercise operations such as change of setpoints, instrument calibration, equipment testing, logic bypass operation, and access to other plant operation switches. Keys, passwords, and other security devices as per the requirements of RG 1.152 are used for qualified plant personnel to enter specific rooms, open specific equipment cabinets, get permission to enter specific electronic instrument for calibration, testing, setpoint changes, and gain access to safety system software and data, etc. However, software of safety systems are typically not changeable at the plant site as the safety system software is implemented as firmware (PROM) microprocessor. There is no access to safety system equipment and control via network from nonsafety system equipment.

Repair (IEEE Std. 603, 5.10)

The ESBWR safety I&C systems are designed to allow the timely recognition (such as through periodic self-diagnostic functions), location, replacement (such as through module replacement), repair and adjustment of malfunctioning equipment. The self-diagnostic function will locate the failure to the component level. Through individual channel bypassing, the failure component can be replaced or repaired on line without affecting the safety system protection function, with the trip logic reverted from 2-out-of-4 to 2-out-of-3. Single failure criterion is still maintained.

Identification (IEEE Std. 603, 5.11)

The ESBWR safety I&C system equipment satisfies with the identification requirements as specified in IEEE 603. Color coding is used as one of the major methods of identification. Safety system equipment is distinctly identified for each redundant portion of a safety system and with identifying markings. For digital computer-based system equipment, versions of computer hardware, programs, and software are distinctly identified. Configuration management is implemented to assist system program and software identification. Typically all hardware component or equipment units have identification label or nameplate.

Auxiliary Features (IEEE Std. 603, 5.12)

ESBWR safety I&C system auxiliary supporting features satisfy the requirements of this standard where applicable, such as safety related electrical system equipment of batteries, diesel generators, inverters, etc. Safety I&C systems are supported by four divisions of Class 1E

uninterruptible power supply, and separately, four divisions of instrument power supply. They are also supported by dc batteries in case there is a loss of off-site and on-site AC power.

HVAC is an important auxiliary supporting feature that supports to maintain the necessary environmental conditions for the safety ESBWR I&C equipment. Under normal operating conditions and whenever the diesel generators is available, HVAC is provided to control the temperature/humidity of all I&C equipment in all of the buildings. Under loss of power condition (SBO or other), batteries are provided for continued safety I&C operation for 24 hours or 72 hours (post accident monitoring equipment), and continued operation of the nonsafety I&C equipment for two hours. HVAC will no longer be available to either control building or reactor building equipment (except the control building area as noted below). The safety I&C equipment will be qualified for the expected temperature rise. In the main control room area, battery-operated nonsafety HVAC is provided to allow continued operation of the safety and nonsafety I&C for the approximate two hours of nonsafety battery capacity. Should the nonsafety HVAC (redundant) not be available, safety-related temperature sensors (with 2/4 logic) will trip the control room power that feeds the nonsafety I&C; the safety I&C is qualified for the resulting temperature rise. This scheme is used to protect the C&I equipment and maximize operator comfort. More description of the HVAC design is included in Chapter 9.

Other auxiliary features that support the safety I&C systems functions are designed such that these components will not degrade the safety system below an acceptable level.

Multi-Unit Stations (IEEE Std. 603, 5.13)

The ESBWR standard design submitted for NRC certification is a single-unit plant.

Human Factors Considerations (IEEE Std. 603, 5.14)

In the ESBWR I&C design, human factors are considered at the initial stage and will be considered throughout the design process, following the necessary regulatory and design guidelines (e.g., NUREG-0711), to assure that safety system design goals are met. Since the ESBWR safety I&C system design concept and architecture follows very closely and similar to the design of the ABWR, the ABWR human factors design practices will largely and effectively support the human factor engineering design of the ESBWR safety I&C systems. More specific information on human factor engineering design program, consideration and requirements are included in Chapter 18 and its associated references.

Reliability (IEEE Std. 603, 5.15)

The degree of redundancy, diversity, testability, and quality of the ESBWR safety I&C design is adequate to achieve the functional reliability necessary to perform its function. All equipment is provided under GE's Appendix B quality program. As an example, Section 9 of Reference 7.1-5 describes special quality program aspects related to GE's programmable digital safety-related I&C equipment. BTP-14 will be followed for software development processes to achieve reliable software design and implementation. Design measures to achieve defense against common mode failure have been included in the safety I&C design through many defense in depth and diversity measures including the incorporation of the Diverse Protection system described in Section 7.8. The ESBWR safety I&C system are included in the consideration of the ESBWR Probabilistic Risk Assessment (PRA), referenced in Chapter 19.

Common Cause Failure Criteria (IEEE Std. 603, 5.16)

The ESBWR has included defense in depth and diversity design consideration, and also has included a Diverse Protection System using both manual action and nonsafety diverse systems to provide means to accomplish the function that could otherwise be defeated by the common cause failure such as common mode software failure. The above design measures including the inclusion of the Diverse Protection System meet the requirements of RG 1.152 on common cause failure and the guidance of BTP HICB – 19. More descriptions of the defense against common mode failure and the Diverse Protection system are included in Section 7.8.

7.1.2.3.4 Sense, Command, and Execute Features per IEEE Std. 603

Automatic and Manual control

The ESBWR RPS and SSLC/ESF logics are designed to automatically initiate reactor scram trip and actuate the engineered safety features to mitigate the consequences of anticipated operational occurrences and design basis accidents. Such automatic protection actions are implemented via a 2-out-of-4 voting (of 4 divisions) whenever one or more process variables monitored and measured by the RPS and SSLC/ESF logics (in 4 divisions) reach the scram or ESF actuation setpoint. In the setpoint determination, appropriate setpoint value is selected for each process variable based on GE setpoint methodology that includes margins and errors. Appropriate instrument and equipment response times are also considered in the safety analyses.

The ESBWR safety I&C systems of RPS and SSLC/ESF manual initiation of protective functions at the system-level and division level is available. The manual controls are designed such that the information provided and display content and location are taken into consideration for easy operator access and action in the main control room. No single failure will prevent the initiation of the protection action. Further information regarding the design of manual controls and human factor engineering consideration, as well as plant manual operation procedure requirements, are included in Chapter 18 and its associated references. Additional descriptions of automatic and manual controls at system levels (RPS and SSLC/ESF) are included in Subsections 7.2.1.1, 7.2.1.2, 7.2.1.3, 7.2.1.5, 7.3.1.1, and 7.3.1.2.

Interaction between the Sense and Command Features and Other Systems

The ESBWR safety I&C protection systems are totally separated and independent from the nonsafety control systems such that any failure of nonsafety systems will not affect and will not prevent the safety protection system from performing its safety protection functions. Sensors used by safety I&C systems are not shared by nonsafety control systems. The Safety I&C systems meet the requirements of GDC 24. Additional descriptions of the safety I&C systems of RPS and SSLC/ESF are included in Subsections 7.2.1 and 7.3.4. (The only interface from nonsafety system to safety-related I&C is the data transmission of LPRM gain adjustment factor data from the plant computer system to the LPRM units. However such data transmission to LPRM units needs operator acknowledgment for implementation, and dose not interfere with reactor protection function or ESF actuation function.)

Derivation of system Inputs

To the extent feasible, the protection system inputs are derived from signals that directly measure the designated process variables. The only two RPS sensing inputs that are not direct measures of the variables are the reactor pressure vessel (RPV) water level and the loss of feedwater flow

in the RPS scram logics. The RPV water level is measured by the delta pressure derived from the sensing line with a reference point. This method is a proven technology in BWR application. The loss of feedwater flow variable is represented by the loss of power generation bus signal, because when the power to the feedwater pump motor is lost, the feedwater flow also is immediately lost. The use of loss of power generation bus signal to represent the loss of feedwater flow signal meet the requirements of the safety analysis of Chapter 15. The RPS initiating circuits and SSLC/ESF logics are described in Subsection 7.2.1 and Section 7.3.

Capability for Testing and Calibration

The operational availability of the protection system sensors can be checked by perturbing the monitored variables, by cross-checking between redundant channels that bear a known relationship to each other and that have read-outs available, or introducing and varying a substitute input to the sensor of the same nature as the measured variable.

Operating Bypasses

Operating bypasses are implemented in the ESBWR safety I&C systems such as RPS, NMS, and SSLC. One example of such operating bypasses is associated with the trip function dependence on reactor operating mode. Requirements of IEEE Std. 603 are met by the ESBWR safety I&C operating bypass design. Specific descriptions of safety system operating bypasses are included in Subsection 7.2.1.5, Subsection 7.2.2.2, and Subsection 7.3.4.2.

Maintenance Bypass

Maintenance bypasses capability is incorporated in the design of the safety I&C systems. This is mainly for the purpose of equipment maintenance, testing, and repair of one individual division (channel) with the plant still under operating condition and without initiating any protection functions. Single failure criterion is maintained under such bypass condition. Maintenance bypass is always alarmed or indicated in the main control room. Maintenance bypass for safety I&C systems is typically applied through joystick bypass switch (with exclusive logic) where only one channel (out of four channels) is allowed to be bypassed at any given time. Technical Specification defines the time duration that a specific maintenance bypass condition is allowed to exist. Maintenance bypasses are initiated manually by the plant operator per administrative control. Specific descriptions of safety system maintenance bypasses are included in Subsection 7.2.1.5, Subsection 7.2.2.2, and Subsection 7.3.4.2.

Setpoints

The ESBWR Safety I&C system setpoints are defined, determined, and implemented based on the GE setpoint methodology approved by the NRC, referenced in Reference 7.2-1. This methodology meets the requirements of IEEE Std. 603.

7.1.2.3.5 Power Source Requirements

The ESBWR Safety I&C protection systems are supported by two independent power sources. Four divisions of Class 1E vital (uninterruptible) 120 VAC are used as the primary power source for the SSLC cabinets in which most components of the safety related protection systems are located. Similarly four Divisional Associated 120VAC Instrument and Control Power (ICP) are used as a secondary power source. Two divisions of the vital (uninterruptible) 120 VAC are also used as the power sources for the solenoids of the scram pilot valves. Two divisions of the

250VDC power sources are used for the backup scram valves solenoids, for scram reset permissive logic. Specific descriptions of safety system power sources are included in Subsections 7.2.1.2, 7.2.2.2, and 7.3.1.1, as well as in Chapter 8.

7.1.2.3.6 Additional IEEE Std. 603 Compliance Discussion applicable to RPS

In addition to above general descriptions of compliance to IEEE Std. 603, a more specific discussion on compliance of IEEE Std. 603 by the RPS and its supporting SSLC functions is included in this section. More supporting descriptions of the RPS and SSLC designs that address to the compliance of IEEE Std. 603 are included in Subsections 7.2.1 and 7.3.4.

Safety System Criteria

The RPS, including its SSLC logic, trip actuator logic, and trip actuators, is designed to comply with this requirement through automatic removal of electric power to the CRD scram pilot valve solenoids when a sufficient number of RPS variables exceeds the specified trip setpoint.

Single-Failure Criterion

The RPS has four completely separate divisions with separate sensors whose only interaction is at the trip logic level via optical isolation. The system is in full compliance with the single-failure criterion and Regulatory Guide 1.53

Quality

All RPS and SSLC components and modules and safety-related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extremes of conditions (as applicable) relating to environment, energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation.

Equipment Qualification

Instrument sensors and electrical components of the RPS and interfacing systems which are used for RPS functions are qualified for nuclear safety-related service for the function times and for the environment in which they are located. The RPS electrical Class 1E equipment, including the SSLC controllers and cabinets, is qualified by type test, data from previous operating experience or analysis, or any combination of these three methods to substantiate that all equipment which must operate to provide the safety system actions will be capable of meeting, on a continuing basis, the necessary performance requirements.

System Integrity

All RPS instrument channels, components, supporting SSLC equipment, and safety- related equipment of other systems providing inputs to the RPS are designed to maintain necessary functional capability under the extreme conditions relating to environment, energy supply, malfunctions, and accidents, within which the equipment has been designed and qualified to operate continuously and without degradation. See above Subsection 7.1.2.3.3 for general discussion.

Channel Independence

The RPS and supporting SSLC equipment are designed to assure that the effects of natural phenomena and of normal operation, maintenance, testing and postulated accident conditions on redundant channels, divisions and equipment of the RPS will not result in the loss of the safety function of the system.

The redundant divisions of RPS/SSLC are electrically and physically separated from each other such that (1) no design basis event is capable of damaging equipment in more than one division and (2) no single failure, test, calibration or maintenance operation can prevent the safety function of more than one division.

Instrument channels that provide signals for the same protective function are independent and physically separated to accomplish the decoupling of the effects of unsafe environmental factors, electric transients and physical accident consequences and to reduce the likelihood of interactions between channels during maintenance operations or in the event of channel malfunctions.

Control and Protection System Interaction

The channels for the RPS trip variables are electrically isolated and physically separated from the plant control systems in compliance with this design requirement.

Multiple redundant sensors and channels assure that no single failure can prevent protective action.

Derivation of System Inputs

The following RPS trip variables are direct measures of a reactor overpressure condition, a reactor overpower condition, a reactor instability condition, a gross fuel damage condition, or abnormal conditions within the reactor coolant pressure boundary:

- Reactor vessel low water level trip
- NMS (APRM/OPRM) divisional trip
- NMS (SRNM) divisional trip
- Drywell high pressure trip
- Reactor vessel high pressure trip

Other variables that could affect the RPS scram function itself, are thus monitored to induce scram directly include:

- Low charging pressure to control rod HCU accumulators
- High suppression pool temperature

The detection of MSIV closure and turbine stop valve closure (if a sufficient number of bypass valves do not open in time) is an appropriate variable for the Reactor Protection System. The desired variable is loss of the reactor heat sink; however, isolation (MSIV closure) or stop valve closure is the logical variable to inform that the steam path has been blocked between the reactor and the heat sink.

Due to the normal throttling action of the turbine control valves with changes in the plant power level, measurement of control valve position is not an appropriate variable from which to infer the desired variable, which is rapid loss of the reactor heat sink. Consequently, a measurement related to control valve closure rate is necessary. Protection system design practice has discouraged use of rate-sensing devices for protective purposes. In this instance, it was determined that detection of hydraulic actuator operation would be a more positive means of determining fast closure of the control valves. Loss of hydraulic pressure in the electrohydraulic control (EHC) oil lines, which initiates fast closure of the control valves, is monitored. These measurements provide indication that fast closure of the control valves is imminent. This measurement is adequate and is a proper variable for the protective function, taking into consideration the reliability of the chosen sensors relative to other available sensors and the difficulty in making direct measurements of control valve fast-closure rate.

The Turbine Stop Valve closure and the steam governing Turbine Control Valve fast closure reactor scram is automatically bypassed when reactor power is below a preset setpoint value, or if sufficient number of the bypass valves are opening as indicated by their 10% position sensors.

Capability for Test and Calibration

The RPS and SSLC fully meet this requirement in that they conform with Regulatory Guides 1.22 and 1.118. The four-channel SSLC logic allows cross-checking between channels and the ability to take any one channel out of service during reactor operation. Such a condition is annunciated and automatically causes the channel trip logic to revert from two-out-of-four to two-out-of-three.

Most sensors have a provision for actual testing and calibration during reactor operation. The exceptions are defined as follows:

- During plant operation, the operator can confirm that the MSIV and turbine stop valve limit switches operate during valve motion. Precise calibration of these sensors requires reactor shutdown.
- Independent functional testing of the air header dump valves can be performed during each refueling outage. In addition, operation of at least one valve can be confirmed following each scram occurrence.

Operating Bypasses

Operating bypasses of the RPS system are described in Subsection 7.2.1.5.2. Whenever the applicable conditions for instrumentation scram bypasses are not met, the RPS will automatically accomplish one of the following: prevent the actuation of an operating bypass; remove any active operating bypass; obtain or retain the permissive conditions for the operating bypass; and initiate the protective function.

Maintenance Bypass

Maintenance bypasses of the RPS system are described in Subsection 7.2.1.5.2.

Indication of Bypasses

Although operating bypasses do not require annunciation, certain operating bypasses are annunciated in the MCR. The CRD HCU accumulator low charging water pressure trip operating bypass, the MSIV closure trip operating bypass, the turbine stop and control valve fast

closure trips operating bypass, and the division-of-sensors bypass are individually annunciated to the operator. Individual SRNM and APRM instrument channel bypasses are indicated on displays for each division on the MCR panels.

Multiple Setpoints

All RPS trip variables are fixed except for the following, which are individually addressed.

The trip setpoint of each SRNM channel is generally fixed. However, there is also the scram initiated by intermediate high neutron flux counting level (corresponding to nominally 5E + 5 counts per second). This is only activated in a non-coincidence scram mode by a switch in the NMS cabinet. The conditions under which such trip is to be activated are included in plant operating procedures.

In modes other than RUN, the APRM setdown function automatically selects a more restrictive scram trip setpoint at a fixed lower value (nominally at 15%). The devices used to prevent improper use of the less restrictive setpoints are designed in accordance with criteria regarding performance and reliability of protection system equipment.

Operation of the mode switch from one position to another bypasses various RPS trips and channels and automatically alters NMS trip setpoints in accordance with the reactor conditions implied by the given position of the mode switch. All equipment associated with these setpoint changes are considered part of the protection system and are qualified Class 1E components.

Completion of Protective Action

It is only necessary that the process sensors remain in a tripped condition for a sufficient length of time to trip the digital trip modules and operate the seal-in circuitry, provided the two-out-of-four logic is satisfied. Once this action is accomplished, the trip actuator logic proceeds to initiate reactor scram regardless of the state of the process sensors that initiated the sequence of events. The same holds true for the manual scram pushbuttons.

Manual Control

Two manual scram pushbutton controls are provided on the principal MCR console to permit manual initiation of reactor scram at the system level. Both switches must be depressed to initiate a scram. Backup to these manual controls is provided by the SHUTDOWN position of the reactor system mode switch. Failure of the manual scram portion of the RPS cannot prevent the automatic initiation of protective action, nor can failure of an automatic RPS function prevent the manual portions of the system from initiating the protective action.

No single failure in the manual or automatic portions of the system can prevent either a manual or automatic scram.

Control of Access

The RPS/SSLC design permits the administrative control of access to all setpoint adjustments, module calibration adjustments and test points. These administrative controls are supported by provisions within the safety system design, by provisions in the generating station design, or by a combination of both.

System Status Indication

When any one of the redundant sensor trip modules exceeds its setpoint value for the RPS trip variables, a MCR display is initiated to identify the particular variable. In the case of NMS trips to the RPS, the specific variable or variables that exceed setpoint values are identified as a function of the NMS. Identification of the particular trip channel exceeding its setpoint is accomplished by permanent storage in the plant computer system. When any manual scram pushbutton is depressed, a MCR annunciation is initiated and a plant computer system record is produced to identify the tripped RPS trip logic.

Repair

Generally, all components can be replaced, repaired, and adjusted during operation. Exceptions are listed below.

During periodic testing of the sensor channels for the following trip variables, all defective components can be identified. Replacement and repair of failed sensors can only be accomplished during reactor shutdown.

- Neutron Monitoring System detectors
- Turbine control valve fast closure sensors
- MSIV closure sensors
- Turbine stop valve closure sensors

Provisions have been made to facilitate repair of NMS components during plant operation except for the detectors. Replacement of the detectors can be accomplished during shutdown.

Identification

The RPS logic is housed in the safety system logic and control (SSLC) reactor trip and isolation functions (RTIF) cabinets. There are four distinct and separate cabinets in accordance with the four electrical divisions. Each division is uniquely identified by color code including cables and associated cables. The SSLC cabinets are marked with the words "Safety System Logic and Control." Each of the safety systems controlled is clearly identified on the cabinets in accordance with their system grouping and labeling. MCR panels are identified by tags on the panels, which indicate the function and identify the contained logic channels. Redundant racks are identified by the identification marker plates of instruments on the racks.

7.1.3 COL Information

None.

7.1.4 References

7.1-1 U.S.N.R.C., "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," NUREG-0800.

7.1-2 GE Energy, "SSLC/RTIF System Performance Specification," NEDE-33232P (Proprietary), NEDO-33232 (Non-Proprietary), October 2005.

7.1-3 GE Energy, "Safety System Logic and Control/Reactor Trip and Isolation Functions (SSLC/RTIF) Hardware/Software Specification," NEDE-33233P (Proprietary), NEDO-33233 (Non-Proprietary), October 2005.

7.1-4 GE Energy, "RTIF Digital Trip Module (DTM) Function Software Design Specification," NEDO-33234 (Non-Proprietary), October 2005.

7.1-5 GE Energy, "Nuclear Measurement Analysis and Control Power Range Neutron Monitor (NUMAC PRNM) Retrofit Plus Option III Stability Trip Function," NEDC-32410P-A (Proprietary), October 1995.

7.1-6 GE Nuclear Energy, "The Nuclear Measurement Analysis and Control Wide Range Neutron Monitor System (NUMAC WRNMS)," NEDO-31439-A (Non-Proprietary), October 1990.

7.1-7 General Electric Company, "General Electric Environmental Qualification Program," NEDE-24362-1-P, Revision 1, Class III (proprietary), January 1983.

7.1-8 Electric Power Research Institute, "Guidelines for Electromagnetic Interference Testing in Power Plants," EPRI TR-102323, Final Report, June 1994.

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 1

Applicable Criteria	10 CFR														
	50.55a(a)(1)	50.55a(h)	50.34 (f) (2) (v) (I.D.3)	50.34 (f) (2) (xvii) (II.F.1)	50.34 (f) (2) (xviii) (II.F.2)	50.34 (f) (2) (xiv) (II.E.4.2)	50.34 (f) (2) (xix) (II.F.3)	50.34 (f) (2) (xxiv) (II.K.3.23)	50.62	52.47 (a) (1) (iv)	52.47 (a) (1) (vi)	52.47 (a) (1) (vii)	52.47 (a) (2)	52.47 (b) (2) (i)	52.79 (c)
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A		ANSI/IEE E Std 279	NUREG 718, 737, 694	NUREG 718, 737, 694	NUREG 694	NUREG 737	NUREG 718	NUREG 718		(Tier 2)	(Tier 1)	(Tier 1)	(Tiers 1&2)	(Tier 2)	(Tier 1)
Reactor Protection System	X	X	X							X	X	X	X	X	X
Neutron Monitoring System	X	X	X							X	X	X	X	X	X
Suppression Pool Temperature Monitor Function	X	X	X							X	X	X	X	X	X
Automatic Depressurization System	X	X	X			X				X	X	X	X	X	X
Gravity-Driven Cooling System	X	X	X			X				X	X	X	X	X	X
Leak Detection & Isolation System	X	X	X			X				X	X	X	X	X	X
Safety System Logic & Control System	X	X	X			X				X	X	X	X	X	X
Standby Liquid Control System	X	X								X	X	X	X	X	X
Remote Shutdown System	X	X								X	X	X	X	X	X
Reactor Water Cleanup/Shutdown Cooling System	X	X								X	X	X			X
Isolation Condenser System	X	X								X	X	X	X	X	X
Post Accident Monitoring System	X	X	X	X	X		X	X		X	X	X	X	X	X
Containment Monitoring System	X	X	X	X			X			X	X	X	X	X	X
Process Radiation Monitoring System	X	X	X	X			X			X	X	X	X	X	X
Area Radiation Monitoring System	X	X		X			X			X	X	X			X
Interlock Systems	X	X	X							X	X	X	X	X	X
Nuclear Boiler System	X	X								X	X	X	X	X	X
Rod Control & Information System										X	X	X			X
Feedwater Control System										X	X	X			X
Plant Automation System										X	X	X			X
Steam Bypass & Pressure Control System										X	X	X			X
Neutron Monitoring System (Non-safety portion)										X	X	X			X
Containment Inerting System										X	X	X			X
Diverse Instrumentation & Controls	X	X							X	X	X	X	X		X
Essential Distributed Control & Information System	X	X	X						X	X	X	X	X	X	X
Non-Essential Distributed Control & Info. System	X	X							X	X	X	X			X

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 2

	General Design Criteria (GDC)												SRM to SECY 93-087	
Applicable Criteria	1	2	4	13	19	20	21	22	23	24	25	29	II.Q	II.T
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A				BTP HICB-12		IEEE 603	IEEE 603	IEEE 603	IEEE 603	IEEE 603	IEEE 603		BTP HICB-19	
Reactor Protection System	X	X	X	X	X	X	X	X	X	X	X	X	X	
Neutron Monitoring System	X	X	X	X	X	X	X	X	X	X	X	X	X	
Suppression Pool Temperature Monitor Function	X	X	X	X	X	X	X	X	X	X	X	X	X	
Automatic Depressurization System	X	X	X	X	X	X	X	X	X	X			X	
Gravity-Driven Cooling System	X	X	X	X	X	X	X	X	X	X			X	
Leak Detection & Isolation System	X	X	X	X	X	X	X	X	X	X			X	
Safety System Logic & Control System	X	X	X	X	X	X	X	X	X	X			X	
Standby Liquid Control System	X	X	X	X	X					X				
Remote Shutdown System	X	X	X	X	X					X				
Reactor Water Cleanup/Shutdown Cooling System		X	X	X	X					X				
Isolation Condenser System	X	X	X	X	X					X				
Post Accident Monitoring System	X	X	X	X	X					X				X
Containment Monitoring System	X	X	X	X	X					X				X
Process Radiation Monitoring System	X	X	X	X	X					X				X
Area Radiation Monitoring System		X	X	X	X					X				
Interlock Systems	X	X	X	X	X					X	X			
Nuclear Boiler System	X	X	X	X	X					X			X	
Rod Control & Information System				X	X					X		X		
Feedwater Control System				X	X					X				
Plant Automation System				X	X					X				
Steam Bypass & Pressure Control System				X	X					X				
Neutron Monitoring System (Non-safety portion)				X	X					X				
Containment Inerting System				X	X					X				
Diverse Instrumentation & Controls	X			X	X					X			X	
Essential Distributed Control & Information System	X	X	X	X	X		X	X	X	X		X	X	X
Non-Essential Distributed Control & Info. System				X	X					X				

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 3

Applicable Criteria	Regulatory Guides																
	1.22	1.47	1.53	1.62	1.75	1.97	1.105	1.118	1.151	1.152*	1.153	1.168*	1.169*	1.170*	1.171*	1.172*	1.173*
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A	BTP HICB-8 & 17	IEEE 279	IEEE 379	IEEE 279	IEEE 384	ANSI/ANS 4.5	BTP HICB-12	IEEE 338	ANSI/ISA-S67.02	IEEE 7-4.3.2	IEEE 603	IEEE 1012, 1028	IEEE 828, 1042	IEEE 829	IEEE 1008	IEEE 830	IEEE 1074
Reactor Protection System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Neutron Monitoring System	X	X	X		X		X	X		X	X	X	X	X	X	X	X
Suppression Pool Temperature Monitor Function	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Automatic Depressurization System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Gravity-Driven Cooling System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Leak Detection & Isolation System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Safety System Logic & Control System	X	X	X	X	X		X	X		X	X	X	X	X	X	X	X
Standby Liquid Control System			X		X		X	X		X	X	X	X	X	X	X	X
Remote Shutdown System			X		X			X		X	X	X	X	X	X	X	X
Reactor Water Cleanup/Shutdown Cooling System																	
Isolation Condenser System			X		X		X	X		X	X	X	X	X	X	X	X
Post Accident Monitoring System						X											
Containment Monitoring System		X	X		X		X	X		X	X	X	X	X	X	X	X
Process Radiation Monitoring System		X	X		X		X	X		X	X	X	X	X	X	X	X
Area Radiation Monitoring System																	
Interlock Systems		X	X		X		X	X		X	X	X	X	X	X	X	X
Nuclear Boiler System					X		X		X	X	X	X	X	X	X	X	X
Rod Control & Information System																	
Feedwater Control System																	
Plant Automation System																	
Steam Bypass & Pressure Control System																	
Neutron Monitoring System (Non-safety portion)																	
Containment Inerting System																	
Diverse Instrumentation & Controls	X			X	X		X	X		X	X	X	X	X	X	X	X
Essential Distributed Control & Information System	X	X	X		X		X	X		X	X	X	X	X	X	X	X
Non-Essential Distributed Control & Info. System																	

* These criteria are addressed in conjunction with the Safety System Logic and Control System (SSLC)

Table 7.1-1 Regulatory Requirements Applicability Matrix, Part 4

Applicable Criteria SRP NUREG-0800 App 7-A	Branch Technical Positions (BTP) HICB														
	HICB-1	HICB-3	HICB-6	HICB-8	HICB-9	HICB-10	HICB-11	HICB-12	HICB-13	HICB-14*	HICB-16	HICB-17*	HICB-18*	HICB-19*	HICB-21*
Reference Standard Guidelines: SRP NUREG-0800 App. 7.1-A	RG 1.153	IEEE 603	IEEE 603	RGs 1.22, 1.153	RG 1.153	RG 1.97	RGs 1.75, 1.153	RG 1.105	RG 1.153	RG 1.152	RG 1.70, Tier 1,2	RGs 1.22, 1.153	NUREG/CR-6090	SECY 93-087 II.Q	NUREG/CR-6083
Reactor Protection System		X		X	X		X	X	X	X	X	X	X	X	X
Neutron Monitoring System		X		X			X	X		X	X	X	X	X	X
Suppression Pool Temperature Monitor Function		X		X			X	X	X	X	X	X	X	X	X
Automatic Depressurization System		X	X	X			X	X		X	X	X	X	X	X
Gravity-Driven Cooling System		X	X	X			X	X	X	X	X	X	X	X	X
Leak Detection & Isolation System				X			X	X	X	X	X	X	X	X	X
Safety System Logic & Control System		X	X	X			X	X	X	X	X	X	X	X	X
Standby Liquid Control System							X	X		X	X	X	X		X
Remote Shutdown System							X			X	X	X	X		X
Reactor Water Cleanup/Shutdown Cooling System											X				
Isolation Condenser System							X	X	X	X	X	X	X		X
Post Accident Monitoring						X									
Containment Monitoring System							X	X	X	X	X	X	X		X
Process Radiation Monitoring System							X	X	X	X	X	X	X		X
Area Radiation Monitoring System											X				
Interlock Systems	X						X	X		X	X	X	X		X
Nuclear Boiler System							X	X		X	X	X	X	X	X
Rod Control & Information System											X				
Feedwater Control System											X				
Plant Automation System											X				
Steam Bypass & Pressure Control System											X				
Neutron Monitoring System (Non-safety portion)											X				
Containment Inerting System											X				
Diverse Instrumentation & Controls				X			X	X		X	X	X	X	X	X
Essential Distributed Control & Information System				X			X	X		X	X	X	X	X	X
Non-Essential Distributed Control & Info. System											X				

* These criteria are addressed in conjunction with the Safety System Logic and Control System (SSLC)

Table 7.1-2 Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

IEEE Section #	Subject	SSLC/RTIF	NMS	SSLC/ESF	RSS	PAM	E-DCIS
	Logic function	*RPS, LDIS, SLC*		*ADS, GDCS, ICS*			
5. Safety system criteria							
5.1	Single-failure criterion	7.2.1.1, 7.2.1.2.4, 7.2.1.3, 7.3.3.1, 7.3.3.2, 7.3.3.3	7.2.2.2, 7.2.2.3.2	7.3.1.1.2, 7.3.1.1.3, 7.3.1.2.2, 7.3.1.2.3, 7.3.4.2, 7.7.1.3, 7.8.1.2.2	7.4.2.2	Tab.7.5-1	7.9.1.2, 7.9.1.3
5.2	Completion of protective action	7.2.1.1, 7.2.1.2.4.2, 7.2.1.3, 7.3.3.1		7.3.1.2, 7.3.4.2			
5.3	Quality	7.2.1.3		7.3.4.3		Tab.7.5-1	
5.4	Equipment qualification	7.2.1.3	7.2.2.2, 7.2.2.3.2	7.3.4.3		Tab.7.5-1	
5.5	System integrity	7.2.1.3	7.2.2.1.1, 7.2.2.1.2	7.3.4.3			
5.6	Independence	7.2.1.1, 7.2.1.2.4, 7.2.1.3, 7.3.3.3.2	7.2.2.1, 7.2.2.2, 7.2.2.3	7.3.1.1.3, 7.3.1.2.3, 7.3.4.2, 7.3.4.3	7.4.2.2	Tab.7.5-1	7.9.1.2, 7.9.1.3
5.7	Testing and calibration	7.2.1.3, 7.2.1.4, 7.3.3.3.2	7.2.2.3.2, 7.2.2.4, 7.2.3.4.2	7.3.1.1.3, 7.3.1.1.4, 7.3.1.2.3, 7.3.4.3, 7.3.4.4	7.4.2.4	Tab.7.5-1	7.9.1.2, 7.9.1.3
5.8	Information displays	7.2.1.2.4.3, 7.2.1.3, 7.2.3.3	7.2.2.3.2, 7.2.2.5.1	7.3.1.1.2, 7.3.1.1.5, 7.3.1.2.2, 7.3.1.2.3, 7.3.1.2.4, 7.3.4.5	7.4.2.2, 7.4.2.5	Tab.7.5-1	
5.9	Control of access	7211, 7213, 72152			7.4.2.2	Tab.7.5-1	
5.10	Repair	7.2.1.1, 7.2.1.2.4.4, 7.2.1.4, 7.2.1.5.2, 7.3.3.3	7.2.2.2.1, 7.2.2.2.3	7.3.4.1, 7.3.4.2		Tab.7.5-1	7.9.1.2, 7.9.1.5
5.11	Identification	7.2.1.3		7.3.1.2.3, 7.8.2.2		7512, Tab.7.5-1	
5.12	Auxiliary features	7.2.1.2.3			7.4.2.2	Tab.7.5-1	
5.13	Multi-unit stations	N/A	N/A	N/A	N/A	N/A	N/A
5.14	Human factors	Chapter 18	Chapter 18	Chapter 18		7512,	

Table 7.1-2 Section Roadmap of Evaluation of IEEE Std 603 Specific Criteria Compliance

IEEE Section #	Subject	SSLC/RTIF	NMS	SSLC/ESF	RSS	PAM	E-DCIS
	Logic function	*RPS, LDIS, SLC*		*ADS, GDCS, ICS*			
5. Safety system criteria							
	considerations					Tab.7.5-1	
5.15	Reliability	Chapter 19	Chapter 19	Chapter 19			Chapter 19
5.16	Common cause failure criteria	7.2.1.3, 7.8					

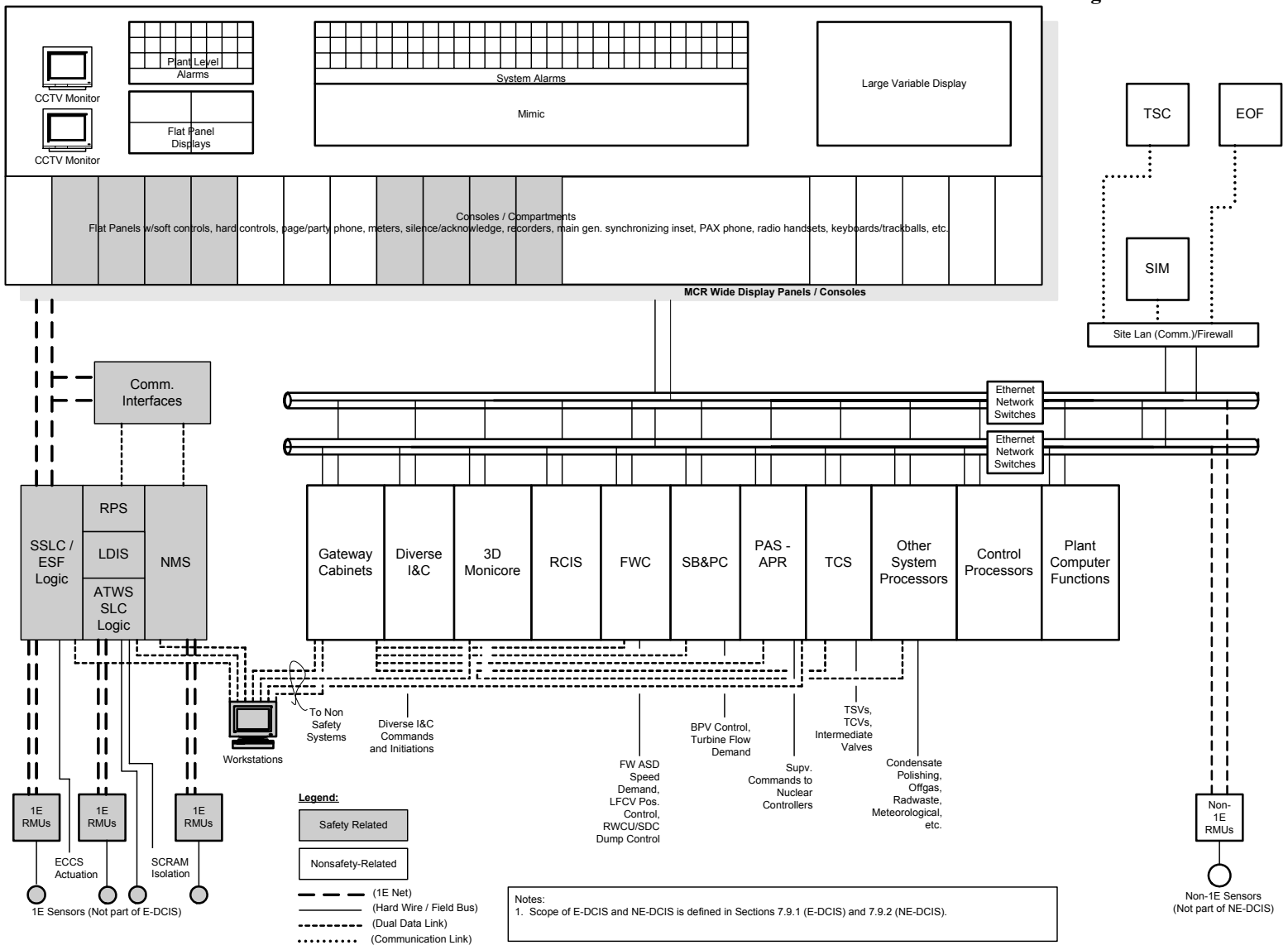
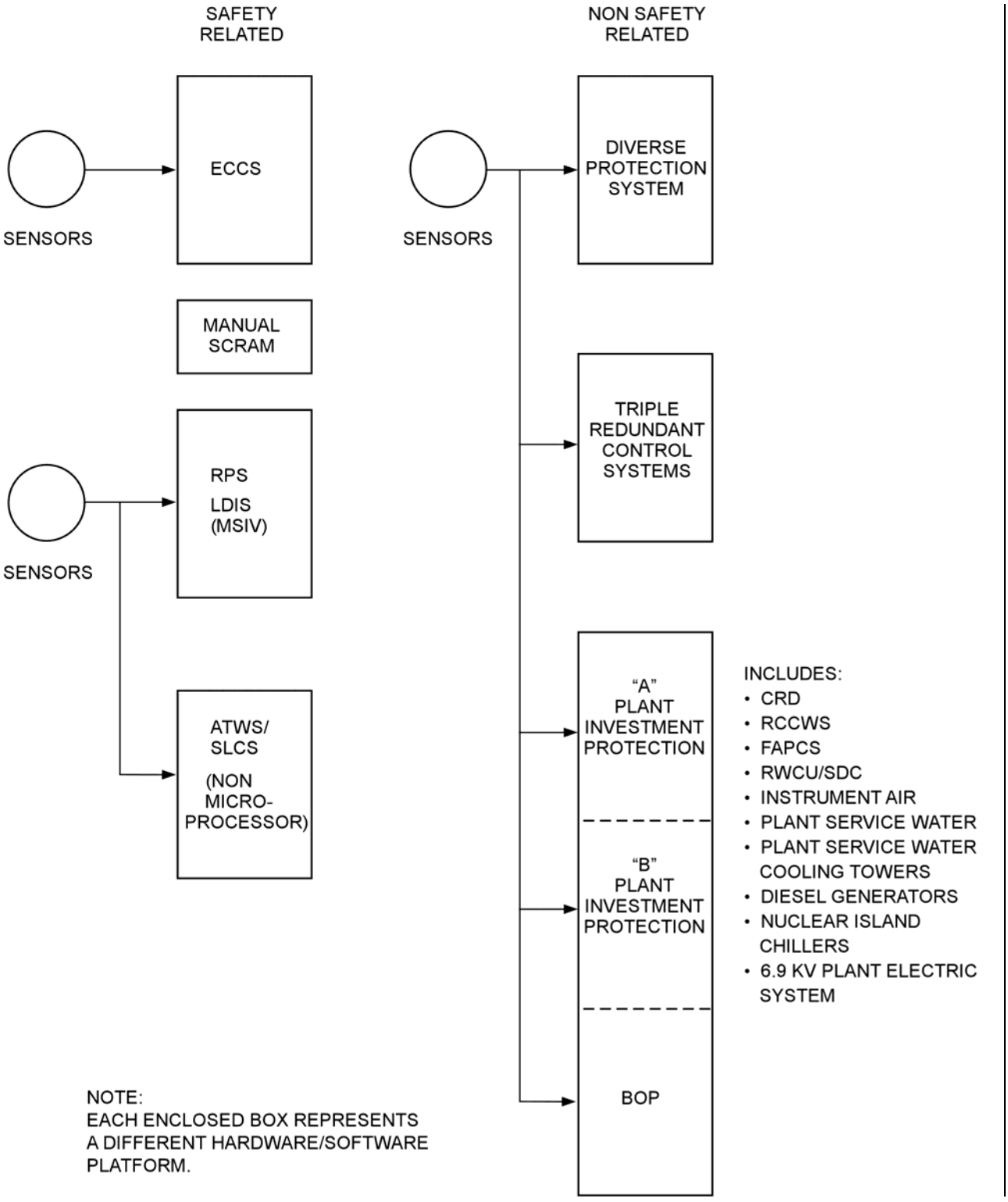


Figure 7.1-1. ESBWR Instrumentation and Control Simplified Block Diagram



(Note: RPS and ATWS/SLC system uses different water level sensors)

Figure 7.1-2. Diversity of ESBWR Instrumentation and Controls

7.2 REACTOR TRIP SYSTEM

7.2.1 Reactor Protection System

7.2.1.1 Design Basis

The Reactor Protection System (RPS) functional requirements are:

(1) To initiate prompt and safe shutdown of the reactor (also known as reactor trip) by means of rapid hydraulic insertion of all control rods (scram):

a. when anticipated operational occurrence (i.e., transient) anomalous states occur, which may impair reactor safety, and

b. when errors in operation take place that lead to transients, which may impair reactor safety.

(1) To provide timely protection against the onset and effects of conditions threatening the integrity of the reactor fuel barriers, the reactor coolant pressure boundary, or the primary containment vessel pressure boundary. This will limit the uncontrolled release of radioactive materials from the fuel assembly or reactor coolant pressure boundary. Also to provide such protection against conditions that threaten important plant equipment integrity.

(2) To initiate an automatic reactor trip whenever monitored process variables exceed or fall below their specified trip setpoints, based on values determined by anticipated operational occurrence (AOO) and accident analyses and instrument setpoint calculation methodology.

(3) To provide manual control switches for initiation of reactor scram by the plant operator when necessary.

(4) To provide mode selection for enabling the appropriate instrument channel trip functions required in a particular mode of plant operation. Mode selection also provides for bypassing instrument channel trip functions that are not required, and for establishing other necessary interlocks associated with the major plant operating modes.

(5) To provide selective automatic and manual operational trip bypasses, as necessary, to permit proper plant operations. These bypasses allow for protection requirements that depend upon specific existing or subsequent reactor operating conditions.

(6) To provide seal-in of specific trip logic paths once trip conditions have been satisfied and also to inhibit the trip reset, as necessary, to ensure subsequent required protective action sequences are completed.

(7) To provide manual reset capability to permit the restoration of the RPS, and other affected systems, to their normal operational status following the seal-in of any trip logic path or after a full reactor scram.

(8) To provide isolated outputs to other systems that share instrument channel signals with the RPS, use trip signals generated by the RPS, or require other indications of specific RPS status for their inputs.

(9) To provide isolated outputs to appropriate warning, trip or bypass alarm annunciators, to operator displays (e.g., flat panel or cathode ray tube CRT displays), and to the plant computer function of the Non-Essential DCIS.

(10) To provide means for calibration and adjustment of trip function setpoints and provide sufficient controls to permit surveillance and post-maintenance testing of RPS equipment.

The following bases ensure that the RPS is designed with sufficient reliability:

(1) Single failures, bypasses, repairs, calibration or adjustments do not impair the normal protective functions of the RPS and do not result in inadvertent reactor scram or insertion of control rods. The RPS is capable of accomplishing its protection functions in the presence of any single failure within the RPS, any failures caused by a single failure, and any failure caused by any design basis event that requires RPS protective action.

(2) The RPS is designed to cause reactor scram even during system shutdown and loss of electrical power sources.

(3) The RPS fails into a safe state if conditions such as disconnection of the system or portions of the system, loss of electrical power, or adverse environment are experienced.

(4) Loss of a single power source directly associated with RPS equipment and protection functions would not cause instrument channel trips or division trips or scram solenoid de-energization that would result in full reactor scram or insertion of any control rod.

(5) Automatically or manually initiated RPS protective actions continue in their intended sequence until completed. RPS output scram signals are maintained until completion of hydraulic control rod insertion.

(6) The RPS has built-in redundancy in its design that satisfies the reliability and availability requirements of the system.

(7) The RPS has bypass capability for failed portions of each division's equipment without degrading operability.

(8) A separate and diverse manual trip function is provided through the use of two manual-trip switches. Actuation of both manual-trip switches is required for a full reactor scram.

(9) Physical separation and electrical isolation between redundant divisions of RPS is provided by separate process instrumentation, separate racks, and separate or independent panels and cabling, and, in the control building, separate equipment rooms.

The following bases reduce the probability that the RPS operational reliability would be degraded by operator error:

(1) Access to trip settings, calibration controls, test points, and other terminal points are under the control of operation supervisory personnel.

(2) Manual bypass of components is under the control of the MCR operator. Any bypass of essential parts of the system is continuously alarmed in the MCR. Physically it shall be possible to insert a bypass into only one channel at a time from the MCR.

(3) Selective automatic and manual trip bypasses are provided to permit proper plant operation.

(4) Manual control switches for initiation of reactor scram, when necessary, by the plant operator, are provided.

(5) Mode selection is provided for enabling the appropriate instrument channel trip functions required in a particular mode of operation.

7.2.1.2 System Description

7.2.1.2.1 RPS Identification

The RPS is the overall complex of instrument channels, trip logics, trip actuators, manual controls and scram logic circuitry that initiate rapid insertion of control rods (scram) to shut down the reactor for situations that could result in unsafe reactor operating conditions. The RPS also establishes appropriate interlocks for different reactor operating modes and provides status and control signals to other systems and alarms. To accomplish its overall function, the RPS interfaces with the Essential Distributed Control & Information System (E-DCIS), Safety System Logic and Control (SSLC), Neutron Monitoring System (NMS), Nuclear Boiler System (NBS), Control Rod Drive System (CRDS), Containment Monitoring System including Suppression Pool Temperature Monitoring (SPTM) function, Rod Control and Information System (RC&IS), Leak Detection and Isolation System (LDIS), Isolation Condenser System (ICS), Steam Bypass and Pressure Control (SBPC) System, Plant Automation System (PAS), Main Control Room Panels, Non-Essential DCIS (NE-DCIS), Uninterruptible AC Power Supply, Instrumentation and Control Power Supply, DC Power Supply, and Raceway System. The RPS sensors, hardware and logic are diverse from both ECCS logic and from the diverse protection system.

A simplified RPS functional block diagram is provided in Figure 7.2-1. A simplified RPS functional block and interface diagram is provided in Figure 7.2-2.

7.2.1.2.2 RPS Classification

The RPS is classified as a safety-related system. The functions and components of the RPS are safety-related unless otherwise indicated. The RPS electrical equipment is also classified as Seismic Category I and as IEEE electrical category Class 1E (Regulatory Guide 1.26 and 10CFR50.55a(h).).

7.2.1.2.3 Power Sources

The RPS logic operates on two types of electrical power, either one of which is capable of supporting RPS operation. Four divisions of vital (uninterruptible) 120 VAC are used as the primary power source for the SSLC cabinets in which most components of the safety related RPS are located. Similarly four Divisional Associated 120VAC Instrument and Control Power (ICP) are used as a secondary power source. Two divisions of the vital (uninterruptible) 120 VAC are also used as the power sources for the solenoids of the scram pilot valves. Two divisions of the 250VDC power sources are used for the backup scram valves solenoids, for scram reset permissive logic, and for initiation logic of the scram-follow electric run-in operation of the nonsafety-related CRD system drive motors.

7.2.1.2.4 RPS Equipment Design

The RPS is designed to provide reliable single-failure-proof capability to automatically or manually initiate a reactor scram while maintaining protection against unnecessary scrams resulting from single failures. The RPS satisfies the single-failure-criterion even when one entire division of channel sensors is bypassed and/or when one of the four automatic RPS trip logic systems is out-of-service. This is accomplished through the combination of fail-safe equipment design, the redundant two-out-of-four sensor channel trip decision logic, and the redundant two-out-of-four trip systems output scram logic arrangement utilized in the SSLC/RPS design. The RPS design satisfies the single failure criterion requirement of IEEE Std. 603.

Equipment within the RPS and within the RPS-related portions of the SSLC is designed to fail into a trip initiating state on loss of power, loss or disconnection of any input signal, or loss of any internal or external device-to-device connection signal. The failure will not affect trip bypass logic signals and trip bypass permissive logic signals.

The design of RPS includes two possible operator controlled bypasses; these are the "division of sensors" bypass and "division of logic (division-out-of-service)" bypass. These are independently controlled by separate fiber optic "joystick" switches that allow the operator to insert the bypass into only one division at a time. There is no combination of operator bypasses that can reduce the redundancy of the RPS system below the requirements of IEEE 279 or IEEE Std. 603; the system will always be able to scram the reactor if any two like and un-bypassed parameters exceed their trip value. Even if RPS back panel chassis are keylock disabled (not an operator function), the required scram capability is maintained. More specifically, there should never be a need to put an RPS channel into "trip".

7.2.1.2.4.1 Arrangement

The RPS-related equipment is divided into four redundant divisions of sensor (instrument) channels, trip logics and trip actuators, and two divisions of manual scram controls and scram logic circuitry. The sensor channels, divisions of trip logic, divisions of trip actuators, and associated portions of the divisions of scram logic circuitry together constitute the RPS automatic scram and air header dump (backup scram) initiation logic. The divisions of manual scram controls and associated portions of the divisions of scram logic circuitry together constitute the RPS manual scram and air header dump initiation logic. The automatic and manual scram initiation logics are independent of each other and use diverse methods and equipment to initiate a reactor scram. Equipment arrangement is shown in Figure 7.2-1.

Sensor Channels - Equipment within a sensor channel consists of sensors (transducers or switches), multiplexers, and functional digital trip modules (DTMs). The sensors within each channel monitor for abnormal operating conditions and send analog (or discrete) output either directly to the RPS cabinets or to Remote Multiplexer Units (RMUs) within the associated division of Essential DCIS. The RMU within each division of E-DCIS performs analog-to-digital conversion on analog signals and sends the digital or digitized analog output values of the monitored variables to the DTM within the associated RPS sensor channel in the same division. The DTM in each sensor channel compares individual monitored variable values with trip setpoint values and for each variable sends a separate (trip/no trip) output signal to the functional Trip Logic Units (TLUs) in the four divisions of trip logic. DTM signals sent from one division to other divisions are optically isolated using optic fiber links. The DTMs and TLUs are

microprocessor-based modules of the SSLC system. The software associated with RPS channel trip and trip system coincident logic decisions that are installed in these SSLC modules are RPS unique. The number of channels utilized in the functional performance of RPS is shown in Table 7.2-1.

E-DCIS and SSLC equipment within a single division of sensor channels are powered from the Class 1E power source of the same division. However, different pieces of equipment may be powered from separate low voltage dc power supplies within the panels belonging to the same division. Within a sensor channel, the sensors themselves may belong to the RPS or may be components of another system. Signal conditioning and distribution performed by the RMUs are functions of the E-DCIS. Components within each of the four RPS sensor channels are totally separated physically and independent from components of other sensor channels, satisfying the independence requirement of IEEE Std. 603. The RPS equipment is independent and physically separated from other safety or nonsafety systems satisfying the requirements of IEEE Std. 603. Any necessary signal communication between the RPS and other systems is through optical isolation devices such as fiber optic cables, via the communication interface module (CIM) of the RPS. There are no signal inputs from other systems that will affect the safety function of the RPS.

Divisions of Trip Logic - Equipment within a RPS division of trip logic consists of trip logic units (TLUs), manual switches, bypass units (BPUs), and output logic units (OLUs). The TLUs, BPUs, and OLUs are functional components of the SSLC system.

The TLUs perform the automatic scram initiation logic, checking for two-out-of-four coincidence of trip conditions in any set of instrument channel signals coming from the four divisions of DTMs or from isolated digital inputs from the four divisions of NMS (trip decisions), and outputting a trip signal if any one of the two-out-of-four coincidence checks is satisfied. The automatic scram initiation logic for any trip is based on the reactor operating mode status and channel trip conditions and bypass conditions. Each TLU, besides receiving isolated digital input trip signals from the four divisions of RPS DTMs, also receives digital input signals from the BPU and other control interfaces in the same division. Signals from one RPS division to another RPS division are electrically isolated using optic fiber cables.

The various manual switches provide the operator with the means to enforce interlocks within RPS trip logic for special operation, maintenance, testing, and system reset. The bypass units perform bypass and interlock logic for the division of channel sensors bypass, and the division trip logic unit bypass. Each SSLC BPU sends a separate bypass signal for the four channels to the TLU in the same division for channel sensors bypass. Each RPS BPU sends the TLU bypass signal to the RPS OLU in the same division.

The OLUs perform division trip, seal-in, reset, and trip test function. Each OLU receives bypass inputs from the RPS BPU, trip inputs from the TLU of the same division, and various manual inputs from switches within the same division. Each OLU provides trip outputs to the trip actuators.

Equipment within a division of trip logic is powered from the same division of Class 1E power source. However, different pieces of equipment may be powered from separate low voltage DC power supplies in the same division.

Divisions of Trip Actuators - Equipment within a division of trip actuators includes isolated load drivers and relays for automatic scram and air header dump initiation. Each division of trip actuators receives trip inputs from the OLU in the same division. The isolated load drivers are solid-state, current-interrupting devices with fast response time. They are powered by 120 VAC and can tolerate the high current levels associated with hydraulic control unit (HCU) scram solenoids operation. The operation of the load drivers is such that a trip signal on the input side creates a high impedance, current interrupting condition on the output side. The output side of each load driver is electrically isolated from its input signal. The load driver outputs are arranged in the scram logic circuitry, which is between the scram solenoids and scram solenoid 120 VAC power source. When in a tripped state, the load drivers cause the scram solenoids (scram initiation) to de-energize. The load drivers within a division interconnect with the OLU of the same division and the OLUs of the other three divisions to form a special arrangement (connected in series and in parallel in two separate groups) that result in two-out-of-four scram logic (i.e., reactor scram occurs if load drivers associated with any two or more divisions receive trip signals) (Figure 7.2-1).

Normally open relay contacts are arranged in the backup scram logic circuitry between the air header dump valve solenoids and 250VDC power source such that, when in a tripped state, the relays cause the air header dump valve solenoids (air header dump initiation) to energize. The relay contacts within a division interconnect with OLUs into two separate two-out-of-four air header dump logic arrangements. Associated relay logic is also utilized to effect scram-follow initiation.

Divisions of Manual Scram Controls - Equipment within a division of manual scram controls includes manual switches, contactors, and relays that provide an alternate, diverse, manual means to initiate a scram and air header dump. Each division's manual scram function controls the power sources to the same division of scram logic circuitry for scram initiation and division of scram logic circuitry for air header dump initiation.

Divisions of Scram Logic Circuitry - One of the two divisions of scram logic circuitry distributes one division of UPS 120 VAC power to the A solenoids of the HCUs and one division of 250VDC power to the solenoid of one of the two air header dump valves. The other division of scram logic circuitry distributes another division of UPS 120 VAC power to the B solenoids of the HCUs and another division of 250VDC power to the solenoid of the other air header dump valve. The HCUs (which include the scram pilot valves and the scram valves) and the air header dump (backup scram) valves are, themselves, components of the CRD system. The arrangement of equipment groups within the RPS from sensors to actuator loads is shown in the Figure 7.2-1. The RPS functional block diagram showing the RPS functions and interfaces with other systems is shown on the Figure 7.2-2.

7.2.1.2.4.2 Initiating Circuits

The RPS logic initiates a reactor scram in the individual sensor channels when any one or more of the conditions listed below exist within the plant during different conditions of reactor operation. The system monitoring the process condition is indicated in brackets.

- High Drywell Pressure [Containment Monitoring System, (CMS)]
- Turbine Stop Valve Closure [RPS]

- Turbine Control Valve Fast Closure [RPS]
- NMS-monitored SRNM and APRM conditions exceed acceptable limits [NMS]
- High Reactor Pressure [NBS]
- Low Reactor Water Level (Level 3) [NBS]
- High Reactor Water Level (Level 8) [NBS]
- Main Steam Line Isolation Valve (MSIV) Closure (RUN mode only) [NBS]
- Low Control Rod Drive HCU Accumulator Charging Header Pressure [CRD system]
- High Suppression Pool Temperature [CMS]
- High Condenser Pressure [RPS]
- Loss of Power Generation Bus (Loss of Feedwater Flow)(RUN mode only) [RPS]
- Operator-initiated Manual Scram [RPS]
- Reactor Mode Switch in "Shutdown" position [RPS]

With the exception of the NMS outputs, the MSIV closure, turbine stop valve closure and turbine control valve fast closure, loss of feedwater flow due to loss of power generation bus, main condenser pressure high, and Manual Scram outputs, which are provided directly to the RPS by dedicated fiber-optic or hard-wired signals, the rest of these systems provide sensor outputs through the Essential Distributed Control & Information System (E-DCIS). The systems and equipment that provide trip and scram initiating inputs to the RPS for these conditions are discussed in the following subsections.

Neutron Monitoring System (NMS)

Separate, isolated, digital Startup Range Neutron Monitor (SRNM) trip signal and Average Power Range Monitor (APRM) trip signal from each of the four divisions of NMS equipment are provided to the four divisions of RPS trip logic, as shown on Figure 7.2-1.

SRNM Trip Signals - The SRNM subsystem provides trip signals to the RPS to cover the range of plant operation from source range through startup range (i.e., more than 10% of reactor rated power). Three SRNM conditions, monitored as a function of the NMS, comprise the SRNM trip logic output to the RPS. These conditions are as follows:

- SRNM upscale (high count rate or high flux level);
- Short (fast) period; and
- SRNM inoperative.

The three trip conditions from every SRNM associated with the same NMS division are combined into a single SRNM trip signal for that division. The specific condition that causes the SRNM trip output state is identified by the NMS and is not detectable within the RPS. The SRNM trip functions are summarized in Table 7.2-2.

APRM Trip Signals - The APRMs provide trip signals to the RPS to cover the range of plant operation from a few percent to greater than rated power. Three APRM conditions, monitored as

a function of the NMS, comprise the APRM trip logic output to the RPS. These conditions are as follows:

- APRM high neutron flux;
- High simulated thermal power; and
- APRM inoperative.

The APRM trip functions are summarized in Table 7.2-3.

Within the APRM subsystem, there is the oscillation power range monitor (OPRM) function that is capable of generating a trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability in time to prevent safety thermal limit violation and fuel damage. This OPRM trip signal is combined with the other three APRM trip signals to form the final APRM trip signal to RPS. The NMS also provides the RPS with a simulated thermal power signal to support the load rejection bypass algorithm.

Nuclear Boiler System

Reactor Pressure - Reactor pressure is measured by four physically separate pressure transmitters mounted on separate divisional local racks in the safety envelope within the reactor building. Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the E-DCIS, which in turn provides the equivalent digital signal to the appropriate SSLC DTM in one of the four RPS divisional sensor channels. The four pressure transmitters and associated instrument lines are components of the NBS.

Reactor Water Level - Reactor water level is measured by four physically separate level (differential pressure) transmitters mounted on separate divisional local racks in the safety envelope within the reactor building. Each transmitter is on a separate pair of instrument lines and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the E-DCIS, which in turn provides the equivalent digital signal to the appropriate SSLC DTM in one of the four RPS divisional sensor channels. The four level transmitters and associated instrument lines are components of the NBS.

Main Steamline Isolation Valve Closure - Each of the four main steam lines (MSLs) can be isolated by closing either its inboard or outboard isolation valve. Position (limit) switches mounted on both isolation valves of each MSL provide outputs, which are hard-wired to the appropriate SSLC DTM in one of the four RPS divisional sensor channels. On each MSL, two position switches are mounted on each of the inboard isolation valve and the outboard isolation valve. Each of the two position switches on any one MSL isolation valve is associated with a different RPS divisional sensor channel. The eight MSIVs and the sixteen position switches supplied with these valves, for RPS use, are components of the NBS.

Control Rod Drive (CRD) System

Locally mounted pressure transmitters measure the CRD system accumulator charging header pressure at four physically separated locations. Each transmitter is associated with a separate RPS division and is on a separate instrument line. Each transmitter provides an analog output signal to the E-DCIS, which in turn provides the equivalent digital signal to the appropriate SSLC DTM in one of the four RPS divisional sensor channels. A RPS scram initiation signal is

generated if the pressure value is below the setpoint value in two (or more) of the four divisions. The four pressure transmitters and associated instrument lines are components of the CRD system.

Reactor Protection System

Turbine Stop Valve Closure - Turbine stop valve (TSV) closure is detected by separate valve stem position switches on each of the four turbine stop valves. Each position switch provides open/close contact output signal through hard-wired connections to the SSLC DTM in one of the four RPS sensor channels. The turbine stop valves are components of main turbine; however, the position switches are components of the RPS.

Turbine Control Valve Fast Closure - Low hydraulic trip system oil pressure, which is indicative of turbine control valve fast closure, is detected by separate pressure transmitters on each of the four turbine control valve hydraulic mechanisms. Each pressure transmitter provides a 4-20 mA signal through hard-wired connections to the SSLC DTM in each of the four RPS sensor channels. The turbine control valve (TCV) hydraulic mechanisms are components of the main turbine; however, the pressure transmitters are components of the RPS.

High Condenser Pressure - High condenser pressure is detected by separate pressure transmitters mounted on the main condenser. Each pressure transmitter provides an analog output signal through hard-wired connections to the SSLC DTM in each of the four RPS sensor channels. The pressure transmitters are components of the RPS. The reactor scram at high condenser pressure will initiate to shut off steam flow to the main condenser to protect the main turbine and to avoid the potential for rupturing the low pressure turbine casing; this is also an anticipatory scram in that high condenser pressure will also trip the main turbine and prevent bypass valve operation.

Loss of Power Generation Bus (Loss of Feedwater Flow) —The plant electrical system has four power generation busses that operate at 13.8 kv. Although normally all four busses are energized, the loads on these busses are arranged such that any three busses are required to support power generation. Specifically these busses supply power for the feedwater pumps and circulating water pumps. In RUN mode, at least three of the four busses must be powered. If the voltage sensor (one per division) on each bus senses a low voltage, indicating that less than three buses are operating, a 2-out-of-4 logic will initiate a scram after a preset delay time. This delay time (less than one second) is to allow the fast transfer from the UAT transformer feed to the RAT transformer feed to restore normal bus voltages. Loss of more than three power generation busses is indicative of loss of the feedwater pumps and flow (it is also indicative of loss of condenser vacuum from the loss of the circulating water pumps). The purpose of this scram on loss of the power generation busses is to mitigate the reactor water level drop to Level 1 following the loss of FW pump function. This scram will terminate additional steam production within the vessel before Level 3 is reached.

Manual Scram - Two manual scram switches and the reactor mode switch each provide diverse means to manually initiate a reactor scram independent of conditions within the sensor channels and divisions of trip logic and trip actuators. Each of the two manual scram switches is associated with one of the two divisions of actuator load power. Both manual scram switches have to be actuated to result in a full scram. There is a separate manual switch in each of the four divisions that provides a means to manually trip all trip actuators in that division. An

alternative manual scram can be accomplished by activating any two (or more) of the four manual divisional trip switches.

Reset Logic:

Once a RPS trip condition exists either automatically or by manual demand, and a scram trip signal is initiated, the trip demand will be sent to the load driver for the actuation of the scram function until the scram (control rod fast insertion) function continues until completion. A reset switch is provided to reset the manual scram in both divisions of manual scram controls. A separate manual switch associated with each division of trip actuators provides means to reset the seal-in at the input of all trip actuators in the same division. After a single division trip, reset is possible after 10 seconds. If a full scram has occurred, reset is inhibited for about 10 seconds to allow sufficient time for scram completion.

After a full scram, the CRD charging header pressure will drop below the trip setpoint, resulting in a trip initiating input to all four divisions of trip logic. While this condition exists, the four divisions of trip logic cannot be reset until the CRD charging pressure trip is manually bypassed in all four divisions and all other trip-initiating conditions have been cleared.

Containment Monitoring System (CMS)

Drywell Pressure - Primary containment (drywell) pressure is measured at four physically separate locations by pressure transmitters located on separate divisional local racks in the safety envelope within the reactor building. Each transmitter is on a separate instrument line and is associated with a separate RPS electrical division. Each transmitter provides an analog output signal to the E-DCIS, which in turn provides the equivalent digital signal to the appropriate SSLC DTM in each of the four RPS division sensor channels. The four pressure transmitters and associated instrument lines are components of the CMS.

Suppression Pool Temperature - Four channels of Class 1E divisional suppression pool temperature signals, each formed by the average value of a group of thermocouples installed evenly (both vertically and azimuthally) inside the suppression pool, provide the suppression pool temperature data for automatic scram initiation. When the established limits of high temperature are exceeded in two of the four divisions, scram initiation is generated. The temperature sensors provide analog output signals to the E-DCIS, which in turn provide the equivalent digital signal to the appropriate SSLC DTM. The temperature sensors and associated instrument lines are components of the CMS. (The suppression pool water level signals are provided along with the suppression pool temperature signals. When water level drops below selected temperature sensors, the exposed sensors are logically bypassed such that only sensors below the water level are utilized to determine the averaged temperature signal to the RPS.)

7.2.1.2.4.3 RPS Outputs to Interfacing Systems

Scram Signals to the CRD System - Reactor trip conditions existing in any two or more of the four RPS automatic trip channels and/or in both RPS manual trip channels cause the output circuits of the RPS, normally supplying power to the solenoids of the scram pilot valves of the CRD system, to be disconnected from power, thus resulting in all control rod insertion and reactor shutdown.

At the same time that the scram pilot valve solenoids are disconnected from power by the RPS trip signals, the two scram air header dump valves of the CRD system (backup scram valves) are

actuated by the RPS trip signals to exhaust the air from the scram air header, resulting in backup scram action.

RPS Status Outputs to the NMS - Two types of RPS status condition signals (four combined signals each, one per division) are provided to the NMS by the RPS. Isolated output signals, indicating that the Reactor Mode Switch is in the RUN mode position, are provided to the four divisions of the NMS whenever the mode switch is in that position. These signals are used by the NMS to bypass the NMS SRNM alarm and trip functions whenever the mode switch is in the RUN mode position.

Scram-Follow Signals to the RC&IS - Upon the occurrence of any full reactor scram condition, the RPS provides isolated output signals to the Rod Control and Information System (RC&IS). This enables automatic rod run-in (scram-follow) logic in the RCIS to cause full insertion or "run-in" of the fine motion control rod drives subsequent to scram. The RPS also provides scram test switch status to the RC&IS, indicating the start of a pair-rod scram test, and provides to the RC&IS the status of Reactor Mode Switch position.

Rod Block Signals to the RC&IS - Rod withdrawal inhibit signals (one for each channel) are provided by the RPS by isolated output signals sent to the RC&IS whenever there is a "Low CRD Charging Water Header Pressure" trip signal or any CRD charging pressure trip bypass switch is in the BYPASS position.

Outputs to the LD&IS - The drywell pressure output signals are provided to the Leak Detection and Isolation System (LD&IS) for reactor coolant pressure boundary and primary containment leakage alarm and isolation functions. The drywell pressure output signals are obtained from the RPS sensors (one for each division) and provided to the LD&IS via the E-DCIS. Also, reactor mode switch status signals from each division are provided. RPS also provides an interlock to LDIS for bypassing the MSIV isolation when not in "RUN" mode that would otherwise result from high main condenser vacuum pressure and/or low inlet pressure to the turbine, during startup and shutdown.

Outputs to Main Control Room Panels:

Safety-related status and alarm signals are sent from the RPS to the main operator control console.

Displays **-** Instrument channel sensor checks are capable of being performed at the main control console. Displays exist for readout and comparison of the current values of each set of four (one per division) of the different variables or separate processes being monitored. Displays related to RPS scram variables include the following minimum set of signals:

- Reactor vessel pressure
- Reactor water levels
- Primary containment drywell pressures
- CRD HCU accumulator charging header pressures
- Suppression pool (local or bulk) temperatures
- Power Generation Bus voltages

The values of all scram parameters are continuously sent through isolated gateways to the NE-DCIS where displays of the scram parameters from all divisions are integrated to allow easy comparison between divisions. Additionally the plant computers and alarm systems will alarm should any divisional parameter not agree with the other divisions within a predetermined amount. The intent is that channel sensor checks are being performed continuously.

Alarms - Alarms are provided at the main control console by the trip condition of any of the four sensor trip channels, by the trip condition of each automatic or manual trip system, and by bypassing a scram function. The alarm function is provided through isolated gateways to the plant computer functions.

The following alarms related to RPS status are provided:

- RPS NMS trip (generated in NMS);
- Reactor vessel pressure high;
- Reactor water level low (≤ Level 3);
- Reactor water level high (≥ Level 8);
- Containment (drywell) pressure high;
- MSIV closure trip;
- TSV closure;
- TCV fast closure;
- Main condenser vacuum pressure high
- Loss of Power Generation Bus (Loss of Feedwater Flow)
- CRD HCU accumulator-charging-header-pressure low;
- Suppression pool temperature high;
- RPS divisional automatic trip (auto-scram) (each of the four, i.e., Div. I, II, III, IV automatic trip);
- RPS divisional manual trip (each of the four, i.e., Div. I, II, III, IV manual trip);
- Manual scram trip (two: both Manual A and/or Manual B);
- Mode switch in SHUTDOWN;
- SHUTDOWN mode trip bypassed;
- NON-COINCIDENT NMS trip mode in effect (in NMS);
- NMS trip mode selection switch still in NON-COINCIDENT position with plant in RUN mode (in NMS);
- Division of channel A (or B, C, D) sensors bypassed (four);
- Tripped conditions in Division I (or II, III, IV) and Division I (or II, III, IV) sensors bypassed (four);

- Division I (or II, III, IV) TLU out-of-service bypass (four);
- Bypass of CRD accumulator-charging-header-pressure low trip;
- Any CRD accumulator-charging-header trip, bypass switch still in BYPASS position with plant in STARTUP or RUN mode; and
- Auto-scram test switch in TEST mode (manual trip of automatic logic) (four).

The above RPS displays and alarms satisfy the information display requirements of the IEEE Std. 603.

Outputs to Non-Essential DCIS (Plant Computer Function) - The tripped, bypassed, and reset conditions of the RPS instrument channels, divisions of logic, divisions of trip actuators, and scram logic circuitry, as well as tripped and reset conditions of RPS automatic and manual trip systems, are logged by the plant computer function via gateway connections from Essential DCIS to the Non-Essential DCIS. For conditions that cause reactor trip, NE-DCIS identifies the specific trip variable, the divisional channel identity, and the specific automatic or manual trip system; these signals are also provided to the sequence of events function of the plant computer functions.

Outputs to the Isolation Condenser System (ICS) - Reactor mode switch status (i.e., RUN/NOT-RUN indications) from the four divisions is provided by the RPS to the Isolation Condenser System to be used as automatic operation signal permissives or inhibits. Automatic operation signal permissives are generated whenever the Reactor Mode Switch is placed in the RUN mode positions, and automatic operation signal inhibits are generated whenever the Reactor Mode Switch is placed in any of the remaining three mode positions.

Outputs to the Plant Automation System (PAS) - The RPS provides the PAS with separate signals to indicate the position of the reactor mode switch. The RPS also provides the auto scram signal from the output logic unit to the PAS.

Essential DCIS —RPS employs Essential DCIS to provide four divisionally separated data highways for the analog and discrete sensor inputs to RPS, except some dedicated signals, which are directly hardwired to the RPS. Control outputs from RPS are hardwired.

Uninterruptible AC Power Supply —The AC electric power required by the four divisions of RPS logic is delivered from four physically separate and electrically independent uninterruptible Class 1E 120 V vital AC buses. The power circuits of the "A" and "B" solenoids of the scram pilot valves are powered from two of the four divisional vital AC power supplies.

Instrumentation and Control Power (ICP) Supply - Four divisional associated 120VAC Instrumentation and Control Power (ICP) sources are supplied to RPS cabinets in addition to the uninterruptible AC power sources. Either power source can support RPS operation.

7.2.1.2.4.4 System Logic Architecture & Redundancy

The basic system architecture of the RPS ensures reliable processing of sensed plant variables by employing four independent trip logic systems in four separate divisions of safety protection equipment. Figure 7.2-1 illustrates the basic RPS functional arrangement concept.

Each divisional trip system processes the trip decisions of plant sensor inputs from the four divisions using a 2-out-of-4 coincidence to confirm the final trip state for each variable in each

division. Automatic reactor trip outputs from each system to the final actuators are also confirmed by a 2-out-of-4 coincidence of division trip outputs. A separate and diverse manual trip method is provided in the form of two independent manual trip channels. Actuation of both manual trip systems is required for a full reactor scram. Availability is enhanced that any one division can be bypassed at one time to allow on-line repair without degrading operability. This satisfies the repair requirement of IEEE Std. 603 while maintaining plant availability.

The RPS has built-in redundancy in its design. The RPS consists of four redundant divisions identical in design and independent in operation. Although each division constitutes a separate trip system, normally each division can make 2 out of 4 trip decisions with or without a division of sensors being bypassed. There are four instrument channels provided for each process variable being monitored, one for each RPS division. Four sensors, one per division, are provided for each variable. When more than four sensors are required to monitor a variable, the outputs of the sensors are combined into only four instrument channels. The logic in each division does not depend on absolute time of day and is asynchronous; no division depends on the correct operation of another division. There is no combination of main control room initiated bypasses that can degrade RPS protection below that required.

7.2.1.3 Safety Evaluation

10 CFR Parts 50 and 52:

50.55a(a)(1) "Quality Standards for Systems Important to Safety"

Conformance: The RPS conforms to these criteria, as shown by the following commitments to applicable regulatory guides and standards.

50.55a(h) "Protection Systems," compliance with ANS/IEEE Std 279

Conformance: IEEE Std 603 supercedes IEEE Std 279. Addressing RG 1.153 and IEEE 603, as discussed in Subsections 7.1.2.3.3, 7.1.2.3.6 and 7.2.1.2.4, satisfies 10 CFR 50.55a(h) and IEEE Std 603.

50.34(f)(2)(v) [I.D.3] Bypass and Inoperable Status Indication

Conformance: The RPS design of bypass and inoperable status indication conforms to these requirements, and is consistent with the conformance of the RPS design with the Regulatory Guide 1.47 discussed in this section. It also conforms to the requirements of control and protection system interaction as described in IEEE 603.

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

52.47(a)(1)(vii) Interface Requirements

Conformance: Interface material is provided in Tier 1.

52.47(a)(2) Level of Detail

Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this requirement.

52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

52.79(c), ITAAC in Combined License Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria (GDC):

In accordance with the Standard Review Plan and with Table 7.1-1, the following GDC are addressed for the RPS:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29.
  - Conformance: The RPS is in conformance with the GDC identified above.

Staff Requirements Memoranda*:*

- Item II.Q of SECY-93-087 (Defense Against Common-Mode Failures in Digital Instrument and Control Systems).
- Conformance: In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this SRM, the ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform with the Item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8.

Regulatory Guides

Regulatory Guide 1.22, Periodic Testing of Protection System Actuation Functions - This includes conformance with BTP HICB-8.

The system is capable of being tested during plant operation from sensor device to final actuator device. The tests must be performed in overlapping stages so that an actual reactor scram would not occur as a result of the testing.

Regulatory Guide 1.47, Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems —

- Automatic indication that a system is out of service is provided in the control room. Indicators indicate which part of a system is not operable.
- Annunciator test switches are provided in the control room.
- Individual indicators are arranged together in the control room to indicate which function of the system is out of service, bypassed, or otherwise inoperable. These automatic indicators remain available and cannot be cleared until the function is operable.
- A manual switch or push button is provided for manual bypass actuation, which annunciates out-of-service conditions.

- These display provisions serve to supplement administrative controls and aid the operator in assessing the availability of component and system level protective actions. These displays do not perform a safety-related function.
- System out-of-service alarm circuits are electrically isolated from the plant safety-related systems to prevent adverse effects.
- Testing is included on a periodic basis, when equipment associated with the display is tested.

Regulatory Guide 1.53, Application of the Single-Failure Criterion to Nuclear Power Plant Protection Systems - Compliance with NRC Regulatory Guide 1.53 is satisfied by specifying, designing, and constructing the RPS to meet the single-failure criterion, Section 5.1, of IEEE 603, Standard Criteria for Safety Systems for Nuclear Power Generating Stations, and IEEE 379, Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Class 1E systems. Redundant sensors are used and the logic is arranged to ensure that a failure in a sensing element or the decision logic or an actuator would not prevent protective action. Separated channels are employed so that a fault affecting one channel would not prevent the other channels from operating properly.

Regulatory Guide 1.62, Manual Initiation of Protective Actions - Means are provided for manual initiation of reactor scram through the use of two armed pushbutton switches and the reactor mode switch. Reactor scram is accomplished by operation of both pushbutton switches, or placing the mode switch in the SHUTDOWN position. These switches are located on the main control console.

The amount of equipment common to initiation of both manual scram and automatic scram is limited to actuator load power sources, actuator loads and cabling between the two. There is no shared trip or scram logic equipment for manual scram and automatic scram. No single failure in the manual, automatic, or common portions of the protection system would prevent initiation of reactor scram by manual or automatic means.

Manual initiation of reactor scram, once initiated, goes to completion as required by IEEE 603, Section 5.2.

Regulatory Guide 1.75, Physical Independence of Electric Systems - The RPS complies with the criteria set forth in IEEE 603, Paragraph 5.6, and Regulatory Guide 1.75, which endorses IEEE 384. Class 1E circuits and Class 1E-associated circuits are identified and separated from redundant and non-Class 1E circuits. Isolation devices are provided where an interface exists between redundant Class 1E divisions and between Class 1E or Class 1E-associated circuits and non-Class 1E circuits.

Physical and electrical independence of the instrumentation devices of the system is provided by channel independence for sensors exposed to each process variable. Separate and independent raceways are routed from each device to the respective data acquisition and signal conditioning units (e.g., remote multiplexing unit). Each channel utilizes its own divisional separate and independent electronic equipment located in separate equipment rooms. Trip logic outputs are separated in the same manner as the channels. Signals between redundant RPS divisions are electrically and physically isolated by Class 1E isolators or by fiber optic cables.

Regulatory Guide 1.105, Instrument Setpoints for Safety-Related Systems - The RPS-initiation setpoints are established consistent with this guide. A licensing topical report (Reference 7.2-1) provides a detailed description of this methodology.

Regulatory Guide 1.118, Periodic Testing of Electric Power and Protection System - The RPS complies with RG 1.118 as amplified in IEEE 338. The RPS is designed so that its individual elements can be periodically and independently tested to demonstrate that the system reliability is being maintained. Safety-related RPS equipment allows for inspection and testing during periodic shutdowns and refueling.

Regulatory Position C.5 for APRM - With respect to conformance to position C.5, the inherent time response of the in-core sensors used for the APRM function (fission detectors operating in the ionization chamber mode) is many orders of magnitude faster than the APRM channel response time requirements and the signal conditioning electronics. The sensors cannot be tested without disconnecting and reconnecting to special equipment.

RG 1.152, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants - The RPS fully complies with this regulatory guide. The hardware and software within SSLC for the RPS function and other safety systems are developed in compliance with this Reg. Guide, which endorses IEEE Std. 7-4.3.2. The structured development plan for SSLC controllers includes conformance to all software standards referenced in IEEE Std. 7-4.3.2. Hardware and software are integrated into a final assembly that is validated by testing against input requirements.

RG 1.153, Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The configuration of SSLC regarding independence, separation, and the single-failure criterion for the RPS function and other safety systems conforms to the requirements of this Regulatory Guide which endorses IEEE-Std. 603.

RG 1.168, Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.169, Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.170, Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.171, Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.172, Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.173, Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

Branch Technical Positions

BTP HICB-3: Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service— The ESBWR has no coolant pump and the BTP Position One does not apply to ESBWR. The ESBWR complies with the BTP Position Two.

BTP HICB-8: Guidance for Application of Regulatory Guide 1.22 - The RPS design conforms to this BTP as discussed in the compliance with RG 1.22 in this section.

BTP HICB-9: Guidance on Requirements for Reactor Protection System Anticipatory Trips — Hardware used to provide trip signals in the RPS is designed in accordance with IEEE 603 and is **considered safety-related and meets seismic design requirement as Seismic Category I.**

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices— The RPS design conforms to this position. The RPS and the SSLC logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

Certain diverse and hardwired portions of RPS may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested per the guidelines of Reg. Guide 1.75 and Reg. Guide 1.153.

BTP HICB-12: Guidance on Establishing and Maintaining Instrument Setpoints - The RPS design conforms to this position. The RPS trip setpoints will be consistent with the requirements of Regulatory Guide 1.105. The setpoints will be established based on instrument accuracy, calibration capability and design drift (estimated) allowance data, and will be within the instrument best accuracy range. The digital RPS trip setpoints do not drift and are reported to the NE-DCIS to be alarmed for any change; the analog to digital converters are self calibrating and the RPS uses self diagnostics – all of which are reported to the NE-DCIS through isolated gateways. It is expected that all of the variability in the parameter channel will be attributable to the field sensor. The established setpoints will provide margin to satisfy both safety requirements and plant availability objectives. (See reference 7.2-1.)

BTP HICB-13: Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors - The RPS uses sensor inputs for suppression pool temperature monitoring, which is based on thermocouple type temperature sensor and which is for trip or not trip application, not used for continuous temperature measurement. This BTP does not apply to RPS.

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems

Development of software for the safety system functions within RPS and SSLC conforms to the guidance of this BTP. Discussion of software development is included in the Appendix 7B of this chapter. Safety-related software to be embedded in the memory of the RPS and SSLC controllers is developed according to a structured plan as described in Appendix 7B. These plans follow the software life cycle process described in the BTP.

BTP HICB-16: Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52 - This BTP is applicable to all section of the DCD including this section on RPS. The RPS section content conforms to this BTP.

BTP HICB-17: Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems. The RPS and SSLC controllers conform to this BTP. Discussions on self-test and surveillance tests of RPS and SSLC are provided in Subsections 7.2.1.4 and 7.3.4.4.

BTP HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems

Any portions of RPS and SSLC design that will use commercial grade programmable logic controllers (PLCs) for safety-related functions conform to this BTP (and to BTPs 14, 17, and 21). Such PLCs will be qualified to a level commensurate with safety system requirements.

BTP HICB-19: Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087) - In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this BTP, the ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform with this BTP by the implementation of an additional diverse instrumentation and control system, the DPS, described in Section 7.8.

BTP HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance

The real-time performance of RPS and SSLC in meeting the requirements for safety system trip and initiation response conforms to this BTP. Each RPS or SSLC controller operates independently and asynchronously with respect to other controllers so that timing can readily be evaluated from input to output of each controller. Timing signals are not exchanged between divisions of independent equipment or between controllers within a division.

7.2.1.4 Testing and Inspection Requirements

System Testing: Operational Verifiability

The RPS is designed so that its individual operating elements can be periodically and independently tested to demonstrate that RPS reliability is being maintained.

The RPS design (and the design of other systems providing the RPS with instrument channel inputs) permits verifying, with a high degree of confidence, and during reactor operation, the operational availability of each of the input sensors utilized by the RPS (i.e., channel checks continuously performed by the plant computer function).

The instrument channels are periodically calibrated and adjusted to verify that necessary precision and accuracy is being maintained. Such periodic checking and testing during plant operation is possible without loss of scram capability and without causing an inadvertent scram.

Safety-related RPS equipment is designed to allow inspection and testing during periodic shutdowns of the nuclear reactor and during refueling shutdowns.

Surveillance Testing and In-Service Inspection

The RPS equipment testing includes the following:

- Equipment qualification testing;
- Pre-operational, startup and refueling/outage inspection testing; and

- In-service and operational surveillance testing.

Surveillance Testing - The RPS is designed to permit testing of emergency reactor shutdown by methods simulating actual plant operation and duplicating, as closely as possible, the performance of protective actions, even during reactor operation. These test methods support in-service verification of scram capability with high reliability. To the extent practicable, the RPS components and testing strategies are designed so that identifiable failures are detectable. Test methods are designed to facilitate recognition and location of malfunctioning components so that they may be replaced, adjusted, or repaired. The following surveillance testing is performed:

- **Channel Checks:** Cross comparison of values of analog scram variables, permitting verification of operational availability of sensor instrument channel. These tests are continuously performed by the plant computer function in addition to allowing the operator to perform the verification.
- **Detector Actuation Tests:** Simulated signals input to the individual detectors or sensor channels for RPS-related instrumentation channels, which are similar to actual trip signals capable of initiating a reactor scram, permit the trip channels to be tested or calibrated and setpoints to be verified. This includes the test of both the DTM function and the TLU function. The trip setpoints are continually monitored by the plant computer function in addition to allowing the operator to verify them.
- **Trip System Logic Tests and Trip Actuator Tests:** Simulated scram signals permit trip system logic to be tested, and permit operation of the trip actuators to be tested. A divisional functional test is performed at this level. A divisional functional test or channel functional test provides confidence that the software-based control programs within the SSLC controllers perform as intended. The test is performed by replacing the process signal with a test signal, which is generated by the SSLC test controller instrument. This test checks the function of the digital trip function and checks trip logic and interlock logic response. The function of the DTM is checked with this test. This divisional functional test may be performed on-line with the sensor channel being tested bypassed.
- **Paired-Control-Rods Scram Tests:** Switches are installed in the main control room to permit testing of the fast scram operation of the individual pairs of control rods and to confirm, when necessary, that the individual control rods have scrammed.

Test Intervals - Suitable test intervals for performing in-service tests of the RPS sensor instrument channels and the RPS trip actuators (i.e., load drivers, relays and contactors) are provided in the plant-specific Technical Specifications, as applicable.

Coincident Logic Tests - Testing of coincident two-out-of-four trip logic verifies each combination of trip conditions for each set of input scram variables in an RPS trip channel. Testing also verifies each output logic combination of trip conditions in the four RPS trip systems. This test is performed off-line during plant outage inspection. A comprehensive functional test is performed at this level. The comprehensive test is performed during an outage (with a time interval specified by the Technical Specification). This test verifies overall SSLC system function, computer component function, software and hardware interactions, response times, and error handling in four divisions. This end-to-end test injects test signals in the four divisions at the RMU inputs and to check the 2-out-of-4 voting logic and other controller logics

not checked during divisional functional test or automatic self-diagnostic checks. This test provides assurance that the protective action equipment is within its specified performance characteristics.

7.2.1.5 Instrumentation and Control Requirements

7.2.1.5.1 Automatic Scram Variables

Refer to Subsection 7.2.1.2.4.2 for the automatic scram initiating circuits and the systems that supply to them.

7.2.1.5.2 Automatic and Manual Bypass of Selected Scram Functions

Operational Bypasses

Manual or automatic bypass of certain scram functions permits the selection of suitable plant protection conditions during different conditions of reactor operation. These RPS operational bypasses inhibit actuation of those scram functions not required for a specific state of reactor operation.

The conditions of plant operation that require automatic or manual bypass of certain reactor trip functions are described below:

The turbine stop valve closure trip bypass and control valve fast closure trip operating bypass - To permit continued reactor operation at low-power levels when the turbine stop or control valves are closed. The main steam TSV closure and the steam governing TCV fast closure scram trip functions are automatically bypassed in each division when the reactor power level is below a certain preset power level (bypass setpoint). Also, the TSV closure and TCV fast closure reactor scram is automatically bypassed if a sufficient number of the bypass valves are opened (as indicated by their 10% position sensors) within a preset time delay after the initiation of the reactor trip signal caused by the TCV fast closure or TSV closure. The NMS system sends RPS an analog simulated thermal power signal, which is used to determine both the low power bypass and to determine the required number of bypass valves to open post turbine trip or load rejection. The low power bypass is automatically removed and both scram trip functions enabled at a reactor power level above the bypass setpoint. The bypass permits the RPS to remain in its normal energized state under the specified conditions.

Bypass of scram trip for CRD-accumulator-charging-header low pressure after scram has occurred (alarmed operational bypass) - To permit scram reset, four administratively controlled trip bypass switches are installed in the main control room. This bypass is allowed only when the reactor mode switch is either in “Shutdown” or “Refuel” mode position. When the reactor is in the shutdown or refuel mode, the low CRD HCU accumulator charging header pressure trip can be manually bypassed in each division of trip logic by separate, manual CRD HCU accumulator charging header pressure trip bypass switches. Control of this bypass is achieved with bypass switches through administrative means. This bypass allows RPS reset after a scram while CRD charging header pressure is below the trip setpoint. The low charging water pressure condition would persist until the scram valves are re-closed. Each division of trip logic sends a separate rod withdrawal block signal to the RCIS when this bypass exists in the division. This operational bypass condition is alarmed in the main control room.

The bypass is automatically removed whenever the Reactor Mode Switch is put in either "Startup" or "Run" mode, whether or not the CRD charging pressure bypass switches are in the bypass position. However, a separate alarm would result in the main control room if any of the bypass switches were left in the bypass position when the Reactor Mode Switch is in either "Startup" or "Run" mode.

Bypass of scram trip for main steam isolation valve closure (alarmed operational bypass) - The MSIV closure scram trip function is automatically bypassed in each division whenever the reactor mode switch is in either the SHUTDOWN, REFUEL or STARTUP mode position with reactor pressure in the associated sensor channel less than a predetermined setpoint. This bypass condition is alarmed in the main control room. This bypass permits plant operation when the MSIVs are closed during low power operation. The bypass is automatically removed if the reactor mode switch is moved to the RUN mode position. This bypass permits the RPS to be placed in its normal energized state for operation at low-power levels with the MSIVs closed or not fully open.

Bypass of scram trip for Loss of Power Generation Bus (alarmed operational bypass) - The Loss of Power Generation Bus (Loss of Feedwater Flow) scram trip function is automatically bypassed whenever the reactor mode switch is in either the SHUTDOWN, REFUEL or STARTUP mode position with reactor power less than a predetermined setpoint. This bypass condition is alarmed in the main control room. The bypass is automatically removed if the reactor mode switch is moved to the RUN mode position.

Bypass of scram trip on account of mode switch in SHUTDOWN position (alarmed operational bypass) - The RPS trip caused by the reactor mode switch being placed in the SHUTDOWN mode position is automatically bypassed after a time delay of approximately 10 seconds. This bypass permits resetting of the trip actuators and re-energization of the scram pilot valve solenoids.

Bypass of NMS SRNM trip functions in RUN mode (not alarmed) - Whenever the reactor mode switch is in the RUN mode, SRNM reactor scram trip functions are automatically bypassed. However, this bypass is not alarmed because it is the normal condition in the RUN mode. The SRNM rod block functions are also disabled when the reactor mode switch is in the RUN mode.

Bypass of non-coincident NMS trips in RUN mode - Whenever the reactor mode switch is in the RUN mode position, and if the coincident/non-coincident NMS trip remains in the NON-COINCIDENT position, the non-coincident NMS scram trip functions are automatically disabled (bypassed). This is a NMS function.

The non-coincident NMS trip function is required while core alterations are occurring during initial fuel loading and subsequent refueling operations. During such core alterations, the Reactor Mode Switch is in the REFUEL mode position (or for certain testing conditions, in the SHUTDOWN or STARTUP mode positions). A non-coincident NMS trip will occur in each division of trip logic when any single SRNM trip signal is present in the NMS if the coincident/non-coincident manual switch in the division is in the non-coincident position. This logic is a NMS function.

The non-coincident NMS trip function is automatically removed when the reactor mode switch is in the RUN mode position. If the coincident/non-coincident NMS trip selection switch were in

the NON-COINCIDENT position when the reactor mode switch is in the RUN mode, this would result in an alarm in the main control room. When the reactor is in SHUTDOWN, REFUEL, or STARTUP mode, the non-coincident NMS trip can be manually bypassed by a separate "non-coincident trip disable" switch. These logics are NMS functions.

APRM, OPRM, and SRNM trips have manual bypass capabilities within NMS, not RPS.

Maintenance Bypasses

Manual bypass capability is provided to allow certain portions of RPS-related equipment to be taken out of service for maintenance, repair or replacement. Maintenance bypasses may reduce the degree of redundancy of RPS channels, but does not affect or eliminate any scram function. Protection functions are available while any RPS equipment is in maintenance bypass. Except where indicated otherwise, any maintenance bypass generates a status alarm at the main control room operator's console.

The following maintenance bypasses are provided:

Bypass of detector inputs (Division-Of-Channel-Sensors bypass) (alarmed maintenance bypass) - Manually operated bypass switch with interlock capability (e.g., joystick type switch) is installed in the main control room to bypass (take out of service) the division of channel sensors trip of one RPS division at a time. Whenever a division of channel sensors bypass switch is placed in the bypass position, an alarm occurs in the main control room with an indication of the bypassed channel sensor division. The effect of the channel of sensors bypass is to convert the 2-out-of-4 trip to a 2-out-of-3 trip logic. A channel of sensors bypass in any channel will bypass all trip initiating input signals at the DTM trip input to the TLU. Bypassing a division of sensors will still allow each of the four divisions to determine the 2 out of 3 trip.

This bypass permits any one of the safety-related RPS components of the input sensor channels of one division to be repaired, replaced or maintained, off-line.

RPS trip system output logic bypass TLU output bypass (Division-Out-Of-Service bypass) (alarmed maintenance bypass) - Manually operated bypass switch with interlock capability (e.g., joystick type switch) is installed in the main control room to bypass (take out of service) the RPS trip output logic of one RPS electrical division at a time. This bypass is effective at the TLU trip input to OLU, and permits the SSLC RPS trip logic unit (TLU) of the associated division to be repaired, replaced or maintained off-line.

The interlock ensures that the output signals of only one TLU (of one division) can be bypassed at any one time. Once a bypass of one division of trip logic has been established, bypasses of any of the remaining three division trip logics are inhibited. When a division-out-of-service bypass switch is placed in the BYPASS position, an alarm occurs in the main control room with indication as to which division is out of service. With a division-out-of-service bypass in effect, the operator is still able to manually trip that division.

The division-of-channel-sensors maintenance bypass function and the division-out-of-service maintenance bypass function are independent. Thus, one division of channel sensors may be bypassed (taken out of service at the sensor channels level) and, simultaneously, the same division or any other division may be taken out of service at the RPS trip system level. In all cases the RPS system remains able to trip the reactor if any two (or more) un-bypassed parameters exceed their trip value.

Requirements for Manual Controls

Operator action by means of manual controls is limited to:

- Initiation of scram by manual scram switches;
- Mode switch operation (results in scram if placed in the SHUTDOWN position);
- Reset of automatic trip systems after trip input signals clear;
- Reset of manual trip systems (preferably after reset of the automatic trip systems);
- Manual bypasses for conditions that are specifically permitted; and
- Manual initiation of selected trip systems or trip actuators using trip logic test switches.

Mode Switch

A multi-function, multi-bank, control switch placed on the main control console provides mode selection for the necessary interlocks associated with the various plant modes; namely, SHUTDOWN, REFUEL, STARTUP, and RUN. The switch provides both electrical and physical separation between the sections associated with each of the four separate divisions.

Manual Scram Switches

Two manual scram switches permit initiating a scram independent of conditions within other RPS equipment (sensor channels, divisions of trip logic, or divisions of trip actuators). Each manual scram switch is associated with one of the two divisions of actuator load power. Both manual scram switches are located on the main control console and do not require any microprocessor functionality; these same switches are included in the RSS panels.

Manual Divisional Trip Switches

Each of the four RPS automatic trip systems has manual trip capability provided by four divisional trip switches that are located in positions easily accessible for optional use by the plant operator. Each switch, when momentarily put into its trip position, trips the actuators that normally would be tripped by a scram condition for that division. Note that momentarily operating any two of the four manual divisional trip switches results in a full reactor scram.

Trip Reset Switches

Up to five trip-reset switches reset any of the four automatic and two manual-scram trip systems that may have been tripped and sealed-in, as follows:

One trip reset switch resets both manual trip systems. The switch circuitry staggers the re-energization of the four groups of scram pilot valve solenoids so that only two groups of "A" and "B" solenoids are re-energized at the same time.

Four separate switches comprise the trip-reset function for resetting the sealed-in, automatic trip logic outputs in the four divisions. Thus, physical separation of the four electrical divisions is maintained.

Operational Bypass Switches

Requirements for operational bypass switches for RPS safety-related functions are addressed in Subsection 7.2.1.5.2. Operational bypass switches are under administrative control. Four trip-

bypass switches implement RPS operational bypass switches for CRD charging header pressure, one for each RPS division. The Reactor Mode Switch provides for several automatic operational bypasses.

Reactor Mode Switch-In Shutdown Scram Bypass Switches

Two manual control switches are used to bypass the scram received when moving the reactor mode switch to shutdown position. This bypass would only be permitted during an outage condition when the reactor is already shutdown.

Maintenance Bypass Switches

Requirements for RPS-related maintenance bypass switches are addressed in Subsection 7.2.1.5.2. The following maintenance bypasses are provided:

- Four division-of-channel-sensor maintenance bypass switches; and
- Four division-out-of-service maintenance bypass switches.

Test Switches

Test switches to aid in surveillance testing during reactor operations are provided in the RPS design.

7.2.2 Neutron Monitoring System

7.2.2.1 Design Bases

The Neutron Monitoring System (NMS) monitors thermal neutron flux from the startup source range to beyond rated power. The NMS is comprised of the following subsystems:

- Startup Range Neutron Monitor (SRNM)
- Power Range Neutron Monitor (PRNM)
- Automatic Fixed In-Core Probe (AFIP)
- Multi-Channel Rod Block Monitor (MRBM)

The PRNM subsystem includes the local power range monitor (LPRM), average power range monitor (APRM) functions, and the oscillation power range monitor (OPRM).

The SRNM and PRNM subsystems are safety-related and are discussed below. The nonsafety-related AFIP Subsystem and the MRBM are addressed in Subsection 7.7.6.

7.2.2.1.1 Startup Range Neutron Monitor (SRNM) Subsystem

Safety-Related (10 CFR 50.2) Design Bases

The general functional requirements follow below:

- The SRNM shall be designed as a safety-related system. The SRNM shall generate a high neutron flux trip signal or a short period trip signal that can be used to initiate scram in time to prevent fuel damage resulting from AOOs or infrequent events.
- The SRNM and its preamplifier shall be qualified to operate under design basis accident and abnormal environmental conditions.

- The independence and redundancy incorporated in the SRNM functional design shall be consistent with the safety-related design basis of the RPS.
- The system shall be designed to produce a safety related permissive signal to the ATWS/SLC system logic.

The specific regulatory requirements for the NMS are listed in Table 7.1-1.

Nonsafety-related Design Bases

Neutron sources and neutron detectors together shall result in a signal count rate of at least 3 cps with the control rods fully inserted in a cold unexposed core.

The SRNM is designed to perform the following functions:

- Indicate measurable increases in output signals with the maximum permitted number of SRNM channels out of service during normal reactor startup operations.
- Provide a continuous monitoring of the neutron flux over a range of 10 decades (approximately 1 x 10^3 nv to 1.5 x 10^{13} nv).
- Provide a continuous measure of the time rate of change of neutron flux (reactor period) over the range from -100 seconds to (-) infinity and (+) infinity to +10 seconds.
- Generate interlock signals to block control rod withdrawal if the neutron flux is greater than or less than preset values or if certain electronic failures occur.
- Generate rod block whenever the period decreases below the preset value.
- The loss of a single power bus would not disable the monitoring and alarming functions of the available monitors.

7.2.2.1.2 Local Power Range Monitor (LPRM)

Safety-Related (10 CFR 50.2) Design Bases

The general functional requirements are:

- A sufficient overall number of LPRM signals are provided to satisfy the APRM safety-related design bases.
- The LPRM shall be designed as a safety-related system to satisfy the APRM safety-related design bases.
- The LPRM shall be qualified to operate under design basis accidents and abnormal environmental conditions.

The specific regulatory requirements applicable to the controls and instrumentation for the NMS are shown in Table 7.1-1.

Nonsafety-related Design Bases

The LPRM supplies the following:

- Signals to the APRM that are proportional to the local neutron flux at various locations within the reactor core.
- Signals to alarm high or low local neutron flux.

- Signals proportional to the local neutron flux to drive indicators and displays, and for the Plant computer function used for operator evaluation of power distribution, etc.
- Signals proportional to the local neutron flux for use by other interface systems such as the Rod Control and Information System (RCIS) for the rod block monitoring function.

7.2.2.1.3 Average Power Range Monitor (APRM)

Safety-Related (10 CFR 50.2) Design Bases

The general functional requirements are:

- The APRM shall be designed to safety-related standards. The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the APRM shall be capable of generating a trip signal in response to excessive average neutron flux increases in time to prevent fuel damage. The independence and redundancy incorporated into the design of the APRM shall be consistent with the safety-related design bases of the RPS.
- The system shall be designed to produce a safety related simulated thermal power signal to RPS to allow that system to support reactor power scram bypass requirements.
- The specific regulatory requirements applicable to the controls and instrumentation for the NMS are listed in Table 7.1-1.

Nonsafety-related Design Bases

The APRM provides the following functions:

- A continuous indication of average reactor power (neutron flux) from 1 to 125% of rated reactor power, which overlaps with the SRNM range. Such signals are made available to other interfacing systems as core power information.
- Interlock signals for blocking further rod withdrawal to avoid an unnecessary scram actuation.
- A simulated thermal power signal derived from each APRM channel, which approximates the heat dynamic effects of the fuel.
- A continuous LPRM/APRM display for detection of any neutron flux oscillation in the reactor core.

7.2.2.1.4 Oscillation Power Range Monitor (OPRM)

Safety-Related (10 CFR 50.2) Design Bases

The general functional requirements are:

The OPRM shall be designed to safety-related standards. The general functional requirements are that, under the worst permitted input LPRM bypass conditions, the OPRM shall be capable of generating a trip signal in response to core neutron flux oscillation conditions and thermal-hydraulic instability in time to prevent violation of the thermal safety limit. The independence and redundancy incorporated into the design of the OPRM shall be consistent with the safety-related design bases of the RPS.

Nonsafety-related Design Bases

The OPRM provides core flux oscillation information for plant computer and for main control room display, and alarm when the OPRM is inoperative with insufficient number of LPRM inputs to OPRM.

7.2.2.2 System Description

The safety-related functions of the Neutron Monitoring System (NMS) consist of the Startup Range Neutron Monitor (SRNM) Subsystem, the Local Power Range Monitor (LPRM), the Average Power Range Monitor (APRM), and the Oscillation Power Range Monitor (OPRM). The nonsafety-related Automated Fixed In-Core Probe (AFIP) Subsystem of the Neutron Monitoring System and the Multi-channel Rod Block Monitor (MRBM) are discussed in Subsection 7.7.6. The LPRM and the APRM, with the OPRM, together are also called the Power Range Neutron Monitor (PRNM) Subsystem.

System Identification

The purpose of the NMS is to monitor power generation and, for the safety-related part of the NMS, to provide trip signals to the RPS to initiate reactor scram under excessive neutron flux (and thermal power) levels, excessive neutron flux oscillation, or fast increases in neutron flux (short period). It also provides power information to the Plant Computer and the automated thermal limit monitor (ATLM) in the Rod Control & Information System (RCIS) for control rod block monitoring. The operating range of the various detectors is shown in Figure 7.2-3. A functional block diagram showing a typical SRNM division is shown in Figure 7.2-4. A functional block diagram showing a typical PRNM division is shown in Figure 7.2-5.

Neutron Flux Monitoring Ranges System Safety Classification

The SRNM, LPRM, APRM, and OPRM perform safety-related functions, and have been designed to meet the applicable design criteria. The system is classified as shown in Section 3.2. The safety-related subsystems are qualified in accordance with Sections 3.10 and 3.11.

The AFIP Subsystem of the NMS and the MRBM are nonsafety-related and are discussed within Subsection 7.7.6.

Power Sources

The safety related NMS equipment is powered by the 120 VAC divisional Class 1E Uninterruptible Power Sources (UPS), and 120 VAC divisional associated Instrument and Control Power Supply (ICP). The power sources for each system are discussed in the individual subsystem descriptions.

Startup Range Neutron Monitor (SRNM) Subsystem

General Description

The SRNM monitors neutron flux from the source range ($1x10^3$ nv) to $1.5x10^{13}$ nv. The SRNM subsystem has twelve SRNM channels, each having one fixed in-core regenerative fission chamber sensor.

Power Sources

SRNM channels are powered as listed below:

- A, E, J: 120 VAC Div UPS Bus A (Division I)
- B, F, K: 120 VAC Div UPS Bus B (Division II)
- C, G, L: 120 VAC Div UPS Bus C (Division III)
- D, H, M: 120 VAC Div UPS Bus D (Division IV)

As previously described, each SRNM cabinet is redundantly powered with 120 VAC ICP power from the appropriate division; either source of power can support system operation.

Physical Arrangement

The 12 SRNM detectors are located at fixed elevation about the mid-plane of the fuel region, and are evenly distributed throughout the core. The SRNM locations in the core, together with the neutron source locations, are shown in Figure 7.2-6. Each detector is contained within a pressure barrier dry tube inside the core, with signal output exiting the bottom of the dry tube under-vessel. Detector cables are separated routed to the appropriate containment penetration according to divisional assignment. They are connected to their designated preamplifiers located in the different divisional quadrants of the reactor building. The SRNM preamplifier signals are transmitted to the SRNM digital processing equipment units, which provide algorithms for signal processing and calculation to provide neutron flux, power calculations, period trip margin, period calculations, and provide various outputs for local and control console displays, recorder, and to the plant computer function. As shown in Figure 7.2-4, the individual SRNM channel trips are combined to form a SRNM divisional trip in the NMS Divisional Interface Unit function. This SRNM divisional trip is sent to a SRNM interface unit function in each division that processes the SRNM trip signal of this division with trip inputs from all other three SRNM divisions to form a 2-out-of-4 voting logic. (This is the logic in Coincidence Mode. Further discussion of SRNM trip logic is included in Subsection 7.2.2.5.2.) This final trip output from each of the four divisions is sent to the RPS. Alarm and trip outputs are also provided for both high flux and short period trip or alarm conditions. Such outputs also include the instrument inoperative trip. The electronics for the startup range neutron monitors and their designated bypass units are located in four separate cabinets, one in each of the four divisional reactor building quadrant and in each of the control building divisional equipment room locations. The SRNM satisfies the IEEE Std. 603 single failure criterion that the failure of each individual SRNM channel will not affect the protection function of the SRNM through channel bypasses discussed in the following paragraph. It also satisfies the IEEE Std. 603 independence requirement.

Signal Processing

Over the 10-decade power monitoring range, two monitoring methods are used: (1) the counting method for the lower ranges, which covers from lowest counting range (approximately $1x10^{3}$nv) to $1x10^{9}$nv; and (2) the Campbelling technique (mean square voltage, MSV) for the higher ranges, which cover from $1x10^{8}$nv to $1x\ 10^{13}$nv of neutron flux. In the counting range, the discrete pulses produced by the sensors are applied to a discriminator after pre-amplification. The discriminator, together with other digital noise-limiter features, separates the neutron pulses from gamma radiation and other noise pulses. The neutron pulses are counted. The reactor power is proportional to the count rate. In the MSV range, where it is difficult to distinguish the individual pulses, a DC voltage signal proportional to the mean square value of the input signal is produced. The reactor power is proportional to this mean square voltage. In the mid-range

overlapping region, where the two methods are changed over, the SRNM calculates a neutron flux value based on a weighted interpolation of the two flux values calculated by both methods. A continuous and smooth flux reading transfer is achieved in this manner. There is also the calculation algorithm of the period-based trip circuitry that generates trip margin setpoint for the period trip protection function.

Trip Functions

The SRNM scram trip functions are discussed in Subsection 7.2.1.2.4, and rod block trip functions are discussed in Subsection 7.7.2.2. The SRNM channels also provide trip bypass. The trip setpoints are adjustable. The SRNM trips are shown in Table 7.2-2. A short period signal (the period withdrawal permissive) inhibits continuous control rod withdrawal such that the reactor scram (due to the short reactor period caused by excessive rod withdrawal) can be avoided.

Bypasses and Interlocks

The twelve SRNM channels are divided into four bypass groups. A joystick switch allows only one SRNM at a time to be bypassed in each bypass group; this scheme allows up to four SRNM channels to be bypassed at any one time. There is no additional SRNM bypass capability at the divisional level. However, it is possible to bypass all three SRNMs that belong to the same division. For SRNM calibration or repair, the bypass can be done for each individual channel separately through these SRNM bypasses without putting the whole division out of service. The SRNM subsystem satisfies the repair requirement of IEEE Std. 603. Note that bypassing any of the SRNM sensors within a division does not affect the ability of the divisions to perform 2 out of 4 trip determination using the trip decisions from the divisions. The SRNM subsystem satisfies the IEEE Std. 603 single failure criterion. The SRNM bypass switches are mounted on the control room panel. Bypass functions for the SRNM and the APRM in the NMS are separate (i.e., there is no single NMS divisional bypass that affects both the SRNM and the APRM). Any APRM bypass does not force a SRNM bypass. The individual SRNM power signals are not combined and averaged to form a divisional SRNM power signal. Also, all NMS bypass logic control functions are located within the NMS, not in the RPS.

The SRNM has several major interlock logics. The SRNM trip functions are in effect when the RPS mode switch is not in the RUN position. The SRNM upscale trip setpoint is lowered in the NMS NON-COINCIDENCE mode (Table 7.2-2). The SRNM ATWS Permissive signals are sent to the Safety System Logic Control (SSLC) system as a permissive signal to control initiation of Standby Liquid Control system boron injection and associated functions (e.g., feedwater runback).

Redundancy and Diversity

The signal outputs from the twelve SRNM channels are arranged such that each of the four divisions includes a different set of designated SRNM channels that cover different regions of the core. The SRNM monitoring and protection function is individual channel based. Failure of an un-bypassed single SRNM channel causes an inoperative trip to only one of the four divisions, whereas a full scram requires divisional trips in 2-out-of-4 divisions. Bypassing a single SRNM channel does not cause a trip output to the related SRNM division and would not prevent proper operation of the remaining SRNM channels to perform their safety-related functions (Subsection 7.2.1.2).

Environmental Considerations

The wiring, cables, and connectors located within the drywell are designed for continuous duty in the conditions described in Appendix 3H.

The SRNM instruments are designed to operate under the expected environmental conditions. Environmental qualification is discussed in Section 3.11. Additional information on equipment qualification with respect to environmental considerations is in Reference 7.1-5, Reference 7.1-6, and Reference 7.1-7.

7.2.2.2.2 Local Power Range Monitor

General Description

The Local Power Range Monitor (LPRM) monitors local neutron flux in the power range. The LPRM provides input signals to the APRM (Subsection 7.2.2.2.3), to the RC&IS (Subsection 7.7.2), and to the plant computer function of the NE-DCIS (Subsection 7.9.2).

Uninterruptible Power Supply (UPS)

Alternating current power for the LPRM circuitry is supplied by four divisional 120 VAC UPS buses (A, B, C and D) that correspond to the four safety-related divisions, each LPRM/APRM cabinet is additionally furnished with power from four divisional associated 120 VAC ICP buses; the various cabinets can perform their function with either of the redundant power sources. Each division supplies power to approximately one-fourth of the detectors. Each LPRM detector is provided with a DC power supply, housed in the designated divisional APRM instrument, which furnishes the detector polarizing potential.

Physical Arrangement

A single division of LPRMs consists of a total of sixty-four (64) detectors, taking one detector from each LPRM assembly from a total of 64 assemblies in the core; there are a total of 256 LPRM detectors in the ESBWR core. Each assembly consists of four LPRM fission chamber detectors evenly spaced at four axial positions along the fuel bundle vertical direction. The 64 assemblies are distributed throughout the whole core in evenly spaced locations. Within the core, for each square fuel region of four-by-four fuel bundles, there are four LPRM assemblies located at the four corners of this fuel region. The LPRM detector locations in the core are illustrated in Figure 7.2-7. The LPRM detector axial positions along the fuel bundle vertical direction are illustrated in Figure 7.2-8. The LPRM detector at the lowest position in a detector is designated Position A. Detectors above A are designated B and C, and the uppermost detector is designated D.

The LPRM detector is a fission chamber with a polarizing potential of approximately 100 VDC. The four detectors comprising a detector assembly are contained in a common tube that also houses the automated fixed in-core probe sensors (Subsection 7.7.6). The enclosing housing tube contains holes to allow coolant flow for detector cooling. The whole assembly is installed or removed from the top of the reactor vessel, with the reactor vessel head removed. The upper end of the assembly is held under the top fuel guide plate with a spring plunger. A permanently installed in-core guide tube/housing is located below the lower core plate to confine the assembly, and to provide a sealing surface under the reactor vessel. The LPRM assembly also contains a set of two thermocouples mounted inside the lower portion of the assembly at an

elevation below the core plate. The thermocouple sensors provide core inlet temperature data to be used by the plant computer function of the NE-DCIS (Subsection 7.9.2) for core flow determination using the heat balance method. This pair of thermocouple sensors is mounted on all 64 LPRM assemblies (at the same elevations). Figure 7.2-8 shows the relative elevations of the fixed in-core probe sensors and the thermocouples. The LPRM cables are grouped by associated APRM trip channel under the reactor vessel and routed to the reactor building in conduit to maintain separation. The LPRMs provide inputs to each of the four APRM channels. The four APRM channels are mounted in separate bays with total physical separation. This arrangement and wiring practices provide the required electrical isolation and physical separation, and satisfies the independence requirement of IEEE Std. 603.

Signal Processing

At under-vessel pedestal region, the LPRM detector outputs from the assembly are connected to respective coaxial cables routed through the containment penetrations, and to the signal conditioning units in the reactor building, where the signals are processed, amplified, converted to digital data and transmitted by optic fiber to the control building NMS cabinets located in the safety related equipment rooms. The amplified signal is proportional to the local neutron flux level. The LPRM signals are averaged and normalized to reactor power by the APRM logic to produce an APRM signal (Subsection 7.2.2.2.3). Individual LPRM signals are also transmitted through dedicated interface units in the APRM with proper electrical isolation to other systems such as the RCIS and the Plant Computer, to provide local power information.

Trip Functions

The LPRM channels provide trip and status signals indicating when an LPRM is upscale, downscale, or bypassed.

Bypasses and Interlocks

Each LPRM channel may be individually bypassed. When the maximum allowed number of bypassed LPRMs for each APRM has been exceeded, an inoperative trip is generated by the affected APRM.

Redundancy

The LPRM detectors are assigned in four divisional APRM channels, with 64 LPRM detector signals in each APRM channel. The redundancy criteria are met such that, in the event of a single failure under permissible APRM bypass conditions, the safety-related protection function can still be performed as required.

Environmental Considerations

The LPRM detector and detector assembly are designed to operate up to a gauge pressure of 8.62 MPa (1250 psig) at an ambient temperature of 315°C. The wiring, cables, and connector located within the drywell are designed for continuous duty at drywell ambient conditions. The LPRMs are capable of functioning during and after design basis events, including earthquakes and anticipated operational occurrences (Sections 3.10 and 3.11). Additional information on equipment qualification with respect to environmental considerations is in Reference 7.1-5 and Reference 7.1-7.

7.2.2.2.3 Average Power Range Monitor (APRM)

General Description

The APRMs perform a safety-related function. There are four APRM channels, one per division. Each APRM channel receives 64 LPRM signals through fiber cables from the reactor building as primary inputs, averages the inputs and normalizes the result to provide an APRM value that corresponds to the average core thermal power signal. One APRM channel is associated with each division of the RPS. Each of the divisional NMS trip signals is also sent to the other three RPS divisions through optical isolation.

Power Sources

APRM channels are powered as listed below:

- A: 120 VAC Div UPS Bus A (Division I)
- B: 120 VAC Div UPS Bus B (Division II)
- C: 120 VAC Div UPS Bus C (Division III)
- D: 120 VAC Div UPS Bus D (Division IV)

Each of the four channels is also powered by one of the four divisional associated 120 VAC ICP power, while either of the two redundant power sources will support APRM operation. The bypass units and LPRM detectors associated with each APRM channel receive power from the same power sources as the APRM channel.

Physical Arrangement

The APRM subsystem consists of four independent and separate instrument channels. Each APRM channel consists of sixty-four (64) LPRM signal inputs. The assignment of individual LPRM sensors to each of the four APRM channel is performed such that an even and uniform selection of LPRM sensors from the whole core is realized for each APRM channel. In this manner, the average value of the 64 LPRM signals from the whole core represents the average core power value. The LPRM signals within the APRM channel are averaged and normalized to form an average core power APRM signal. The LPRM assignment to APRM channels is shown in Figure 7.2-9.

Signal Conditioning

The APRM channel electronic equipment averages the output signals from sixty-four LPRM detectors to form an APRM signal for this channel. The averaging circuit automatically corrects for the number of un-bypassed LPRM input signals The APRM channel electronics unit includes the capabilities for LPRM and APRM calibrations and diagnostics. The APRM has signal output interface units in order to send signals to other systems. A simplified PRNM block diagram is shown in Figure 7.2-5. The APRM Interface Unit houses the 2-out-of-4 voter with isolation from the APRM signal conditioning unit. The 2-out-of-4 voter in each division receives trip signals from all four APRM divisions to make the final 2-out-of-4 trip decision. The trip output of the 2-out-of-4 voter is routed to the RPS directly. The APRM satisfies the IEEE Std. 603 single failure criterion that the failure of each individual APRM channel will not affect the protection function of the APRM through channel bypasses discussed in the following paragraph. It also satisfies the IEEE Std. 603 independence requirement, as the redundant

portions of the NMS equipment are independent of and physically separated from each other, and that the NMS equipment is separated from other systems.

Trip Function

The APRM scram trip function is discussed in Subsection 7.2.1.2. The APRM rod block trip function is discussed in Subsection 7.7.2.2. The APRM channels also provide trip and status signals indicating when an APRM channel is upscale, downscale, bypassed, or inoperative. The trip setpoints are adjustable. APRM system trips are summarized in Table 7.2-3. The 2-out-of-4 voter units are physically and electrically separated both from each other and from the APRM/OPRM units to assure independence of the final vote determining the input to the RPS trip systems.

Bypasses and Interlocks

One APRM channel out of four channels may be bypassed at any one time for repair during plant operation while still maintaining the required APRM functions. This satisfied the repair requirement of IEEE Std. 603. When one APRM channel is bypassed, the trip logic to the RPS becomes two-out-of-three instead of two-out-of-four. Each divisional trip signal is sent to all four RPS divisions. All four RPS channels continue to perform the trip logic even if the RPS channel is in the same division as the bypassed APRM input. The bypass of APRM channels is accomplished with a joystick type switch with mutually exclusive positions. The APRM bypass switch is located on the control room panel. Access to the panel and the switch is under administrative control. When a bypass is active, the input from the bypassed APRM/OPRM channel (APRM or OPRM trip function) will be bypassed by removing it from the vote. The remaining signals are voted with a 2-out-of-3 logic, thus retaining the ability to withstand a single channel failure. The final separate check of the signals, performed independently by each voter channel, assures that no single failure will cause an inadvertent bypass. The bypass function uses physical means and independent logic to assure that no more than one channel is bypassed at a given time.

There are no automatic bypasses for the APRM trip function. The APRM trip setpoint is automatically changed to a lower value (setdown) when the manually operated reactor mode switch is not in RUN. When any APRM (or OPRM) channel output to the RPS is bypassed, the bypass is indicated by a light on the plant operator's panel. The same channel bypass bypasses both the OPRM and APRM channel.

Redundancy

Four independent channels of the APRM monitor neutron flux, each channel being associated with one RPS division but with its trip signal being sent to the other three RPS divisions through optical isolation. Any two of the four APRM channels can initiate a reactor trip in any of the RPS channels (i.e., two-out-of-four-logic). The redundancy criteria are met such that in the event of a single failure under permissible APRM bypass conditions, the safety-related protection function can still be performed as required.

Environmental Considerations

Chapter 3 describes the APRM operating environments. The APRM is capable of functioning during and after the design basis events in which continued APRM operation is required

(Sections 3.10 and 3.11). Additional information on equipment qualification with respect to environmental considerations is in Reference 7.1-5 and Reference 7.1-7.

7.2.2.2.4 Oscillation Power Range Monitor

General Description

The Oscillation Power Range Monitor (OPRM) consists of four independent Class 1E channels. The OPRM channel utilizes the same set of LPRM signals used by the associated APRM channel in which this OPRM channel resides. Each OPRM receives the identical LPRM signals from the corresponding APRM channel as inputs, and forms many OPRM cells to monitor the neutron flux behavior of all regions of the core. The LPRM signals assigned to each cell are summed and averaged to provide an OPRM signal for that cell. The OPRM trip protection algorithm detects thermal hydraulic instability (flux oscillation with unacceptable amplitude and frequency) and provides a trip output to the RPS if the trip setpoint is exceeded.

Power Sources

OPRM function resides in the APRM equipment and receives the same redundant APRM power.

Signal Conditioning

The OPRM function resides in its associated APRM channel equipment. Assignment of LPRMs to the four OPRM channels is shown in Figure 7.2-10. The OPRM channel consists of OPRM cells that are formed by grouping LPRM inputs. Each OPRM cell signal is the average of all grouped LPRM input signals for this cell, for detecting thermal hydraulic instability of the reactor core.

Trip Function

The OPRM trips are combined with the APRM trips of the same APRM channel, and sent to RPS. The OPRM function generates an inoperative alarm for an OPRM channel when there is an insufficient number of operating OPRM cells. If the number of operating LPRM inputs to an OPRM cell is less than the minimum required, the cell is considered to be inoperable. Similarly the channel is inoperable if it does not have enough operating cells. Any cell can result in an OPRM channel alarm or trip condition.

Bypasses and Interlocks

The OPRM alarms and trips are bypassed in all reactor operation modes except RUN, and when operating below a preset required power level. The OPRM bypass is controlled by the APRM channel, in which it resides. Bypass of the APRM channel also bypasses the OPRM trip function within this APRM channel.

Redundancy

The OPRM has the same redundancy design as the APRM. The redundancy criteria are met such that in the event of a single failure under permissible APRM/OPRM bypass conditions, the safety-related protection function can still be performed as required.

Environmental Considerations

The OPRM follows the same environmental consideration as the APRM.

7.2.2.3 Safety Evaluation

The evaluation for the trip inputs from the NMS to the RPS is discussed in Subsection 7.2.1.

The AFIP Subsystem and the MRBM are nonsafety-related subsystems of the NMS and are evaluated in Subsection 7.7.6.

This evaluation section covers only the safety-related functions of the NMS. These include the following:

- Startup Range Neutron Monitor (SRNM)
- Local Power Range Monitor (LPRM)
- Average Power Range Monitor (APRM)
- Oscillation Power Range Monitor (OPRM)

7.2.2.3.1 General Functional Requirements Conformance

Startup Range Neutron Monitor

The SRNM is designed as a safety-related subsystem that generates a scram trip signal to prevent fuel damage in the event of any abnormal reactivity insertion transients while operating in the startup power range. This trip signal is generated by either an excessively high neutron flux level, or excessive neutron flux increase rate (i.e., reactor period). The setpoints of these trips are such that under the worst reactivity insertion transients, fuel integrity is always protected. Under the worst bypass condition, where one SRNM from each division is bypassed, the monitoring and protection functions are still adequately provided. The independence and redundancy requirements are incorporated into the design of the SRNM and are consistent with the safety-related design bases of the RPS.

Local Power Range Monitor

The LPRM is designed for monitoring the local power level and to provide a sufficient number of LPRM signals to the APRM system such that the safety-related design basis for the APRM is satisfied. The LPRM itself has no safety-related design basis. However, it is qualified to safety-related standards.

Average Power Range Monitor

The APRM provides information for monitoring the average power level of the reactor core when the reactor power is in the power range. The APRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux increase, in time to prevent fuel damage. Such a trip signal also includes a trip from the simulated thermal power signal, which represents the APRM flux signal through a time constant representing the actual fuel time constant. The resulting simulated thermal power signal accurately represents core thermal (as opposed to neutron flux) power and the heat flux through the fuel. Scram functions are assured when the minimum LPRM input requirement to the APRM is satisfied. If this requirement cannot be met, an inoperative trip signal is generated. The independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

Oscillation Power Range Monitor

The OPRM provides monitoring and protection function for core regional and core wide neutron flux oscillation monitoring, using the same set of LPRM signals used by the associated APRM channel in which the OPRM channel resides. The OPRM is capable of generating a trip signal to scram the reactor in response to excessive and unacceptable neutron flux oscillation, in time to prevent fuel damage. Scram functions are assured when the minimum LPRM input requirement to the OPRM is satisfied. The independence and redundancy requirements are incorporated into the design and are consistent with the safety-related design basis of the RPS.

7.2.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the NMS and the associated codes and standards applied in accordance with the Standard Review Plan. The following evaluation lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50.55a(a)(1) Quality Standard for Systems Important to Safety

Conformance: The NMS conforms to these criteria, as shown by the following commitments to applicable regulatory guides and standards.

10 CFR 50.55a(h) "Protection Systems," compliance with ANS/IEEE Std 279

IEEE Std. 603 is endorsed by Reg. Guide 1.153, superceding the requirements of IEEE Std. 279. Applicable requirements of IEEE 603 are met by the NMS, as described in Subsection 7.1.2.3.3, in Subsection 7.2.2.2, and in this section. The safety-related subsystems of the NMS consist of four divisions, which correspond and interface with those of the RPS. This independence and redundancy assures that no single failure interferes with the system operation. The 2-out-of-4 trip determinations of the NMS are independent of the 2-out-of-4 RPS trip determinations.

The twelve SRNM channels are divided into four divisions; and are independently assigned to four bypass groups such that up to four SRNM channels may be bypassed at any one time while still providing the required monitoring and protection capability.

There are sixty-four LPRM assemblies evenly distributed in the core. There are four LPRM detectors within each LPRM assembly, evenly distributed from near the bottom of the fuel region to near the top of the fuel region (Figure 7.2-8). The two hundred fifty-six detectors are assigned to four divisions that consist of the four APRM channels. Any single LPRM detector is only assigned to one APRM division. Each set of sixty-four LPRM detector signals is assigned to one APRM channel, with these signals averaged and normalized to form an APRM signal the represents the average core power. Electrical and physical separation of the division is thus maintained and optimized to satisfy the safety-related system requirement. With the four divisions, redundancy requirements are met because a scram signal can still be initiated with a postulated single failure of one APRM channel under allowable APRM bypass conditions.

Components used for the safety-related functions are qualified for the environments in which they are located (Section 3.11). Additional information on NMS equipment qualification is included in Reference 7.1-5.Additional reference to the detailed PRNM design compliance to IEEE Std. 603 is included in Reference 7.1-5.

50.34(f)(2)(v) [I.D.3] Bypass and Inoperable Status Indication

The NMS design of bypass and inoperable status indication conforms to this requirement consistent with the conformance of the NMS design with Regulatory Guide 1.47. It also conforms to the requirements of control and protection system interaction as described in IEEE 603.

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

52.47(a)(1)(vii) Interface Requirements

- Conformance: Interface material is provided in Tier 1.

52.47(a)(2) Level of Detail

- Conformance: The level of detail provided for the NMS within the Tier 1 and Tier 2 documents conforms to this requirement.

52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

- Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

52.79(c), ITAAC in Combined License Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria (GDC):

In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, the following GDC are addressed for the NMS:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29.

Conformance: The NMS complies with these GDC, in part, or as a whole, as applicable. The GDC are generically addressed in Section 3.1.

Staff Requirements Memoranda*:*

Item II.Q of SECY-93-087 (Defense Against Common-Mode Failures in Digital Instrument and Control Systems)

- Conformance: The ESBWR NMS design, as part of the safety-related system, conforms to this BTP in conjunction with the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8.

Regulatory Guides (RGs):

In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, the following Regulatory Guides (RGs) are addressed for the NMS:

RG 1.22 - Periodic Testing of Protection System Actuation Functions

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems

RG 1.75 - Physical Independence of Electric Systems

RG 1.105 - Instrument Setpoints for Safety-Related Systems

RG 1.118 - Periodic Testing of Electric Power and Protection Systems

RG 1.152 - Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants

RG 1.153 - Criteria for Power, Instrumentation and Control Portions of Safety Systems

RG 1.168 - Verification, Validation, Reviews and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants

RG 1.169 - Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants

RG 1.170 - Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants

RB 1.171 - Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

RG 1.172 - Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants

RG 1.173 - Developing Software Life cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

The NMS conforms to all the above-listed RGs, using the same interpretations and clarifications identified in Subsections 7.1.2.2 and 7.2.1.3.

Branch Technical Positions (BTPs):

In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, the following BTPs are considered applicable for the NMS:

BTP HICB-3 - Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service

The ESBWR has no coolant pump and the BTP Position One does not apply to ESBWR. The ESBWR complies with the BTP Position Two.

BTP HICB-8 - Guidance for Application of Regulatory Guide 1.22

The NMS is continuously operating during reactor operation. The accuracy of the sensors can be verified by cross-comparison of the various channels within the four redundant divisions and is continuously monitored by and alarmed for inconsistency by the plant computers in NE-DCIS. A minimum number of channels or one division can be bypassed for periodical testing during reactor operation without impacting the NMS in performing the safety function. Therefore, the NMS fully meets this BTP.

BTP HICP-11 - Guidance for Application and Qualification of Isolation Devices

There are four divisional safety-related subsystems of the NMS. Each division is entirely redundant and identical in design, and independent of each other, meeting requirements of IEEE Std. 603. The NMS equipment is protected from disturbance from other interfacing systems and electrical power transient by using fiber optic cables to meet the requirements of RG 1.75 and RG 1.153. The NMS equipment is qualified to requirements of IEEE Std. 323. Hence, the NMS fully meets this BTP.

BTP HICB-12 - Guidance for Establishing and Maintaining Instrument Setpoints

The analytical limits of the safety-related setpoints of the NMS are determined from safety analyses for the reactor fuel each cycle to ensure that the reactor core is protected from any rising neutron flux exceeding these values. The nominal setpoints are calculated to be consistent with the GE standard setpoint methodology, which conforms to RG 1.105 and ISA-S67.04. The setpoint margin calculated by this method has also considered additional uncertainties with the calibration interval. Hence, the NMS fully meets this BTP. Most of the uncertainty associated with safety related NMS trip setpoints is associated with the various neutron sensors since the digital electronics in the NMS does not drift and the setpoints are monitored and alarmed by the plant computer function of NE-DCIS. The plant technical specifications will set a required calibration interval for LPRM detectors and the APRM signals.

BTP HICB-14 - Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems

Development of software for the safety-related system functions within NMS conforms to the guidance of this BTP as discussed in Subsection 7.2.1.3 and Appendix 7B. Safety-related software to be embedded in the memory of the NMS controllers is developed according to a structures plan as described in Appendix 7B. These plans follow the software life cycle process described in the BTP.

BTP HICB-16 - Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

This BTP is applicable to all section of the DCD including this section on NMS. The NMS section content conforms to this BTP.

BTP HICB-17 - Guidance on Self-Test and Surveillance Test Provisions

The safety-related subsystems of the NMS are designed to support the required periodic testing (Refer to Subsection 7.2.2.4). The NMS system equipment is equipped with self-test design operating in all modes of plant operations. This self-test function provides the operator information of equipment failure modes, which would lead to equipment becoming inoperable. This self-test function does not interfere with the safety functions of the system. The NMS meets this BTP.

BTP HICB-18 - Guidance of Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems

Any portions of NMS design that will use commercial grade programmable logic controllers (PLCs) for safety-related functions conform to this BTP. The PLCs will be qualified to a level commensurate with safety system requirements.

BTP HICB-19 - Guidance for Evaluate of Defense-in-Depth and Diversity in Digital Computer-based Instrumentation and Control Systems

NMS is a 4-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment employs non-conductive fiber-optic cable. The four NMS divisions operate asynchronously from each other. System functions are segmented among multiple controllers. Control system functions are separated, independent, and diverse from the protection system. Random failures are mitigated by the divisional channel and channel bypass capability of NMS. A divisional bypass places the remaining divisions in a 2-out-of-3 trip logic condition. The NMS provides trip inputs to the RPS. Design measures to satisfy the Defense-in-Depth and Diversity principles for the RPS and ECCS function are described in Section 7.8.

BTP HICB-21 - Guidance for Digital Computer Real-Time Performance

The SRNM/APRM digital subsystems and the OPRM digital subsystem are designed to respond in real time to ensure that the specified fuel limits are not exceeded, and that core power oscillations are detected and suppressed. The NMS meets this BTP.

TMI Action Plan Requirements - In accordance with the Standard Review Plan for Chapter 7, and with Table 7.1-1, there are no TMI action plan requirements applicable to the NMS.

10 CFR 50.34(f)(2) TMI-Related Requirements: All TMI requirements are addressed within Chapter 1.

7.2.2.4 Testing and Inspection Requirements

7.2.2.4.1 General Requirements

NMS instruments (not including sensors) outside of the containment are designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access to the service personnel.

NMS instrument modules, including SRNM and APRM, are designed with the capability of being tested for the normal performance, trip performance, and calibration function, either through an automated process or through a manual process. Routine surveillance functions, including periodic tests and calibration, are automated with minimum operator interference.

Detailed NMS instrument test function requirements, including periodic tests and calibration durations for each instrument, are included in the detailed NMS hardware and software system specification document.

For microprocessor-based instruments, an instrument unit self-test function is provided.

7.2.2.4.2 Specific Requirements

SRNM Testability and Calibration

Each SRNM channel is tested and calibrated based on the procedures listed in the SRNM instruction manual. Each SRNM channel is checked to ensure that the SRNM high flux scram function and short period scram function are operable.

LPRM Testability and Calibration

LPRM channels are calibrated using data from the AFIP Subsystem and based on Plant computer function three-dimensional core power distribution calculations. The calibration is based on procedures in the applicable instruction manual.

APRM Testability and Calibration

APRM channels are calibrated using data from the Plant computer functions three-dimensional core power and heat balance calculations. The calibration is based on procedures in the applicable instruction manual. Each APRM channel can be tested individually for the operability of the APRM high neutron flux scram and rod-blocking functions by the introduction of test signals.

OPRM Testability and Calibration

Each OPRM channel can be tested individually for the operability of the OPRM Trip Protection algorithm by the introduction of test signals.

7.2.2.5 Instrumentation & Control Requirements

7.2.2.5.1 Instrumentation Requirements

The NMS instruments are primarily based on the digital instrument and control practices with digital design and digital electronics based programmable and memory units. NMS instruments follow a modular design concept such that each modular unit or its subunit is easily replaceable. The instrument has a flexible interface design to accommodate either metal wire or fiber optic communication links.

NMS instruments are provided with necessary operator-interface functions based on adequate NMS man-machine interface requirements.

The required NMS displays provided at the Main Control Room Panel include as a minimum the following:

- SRNM Reactor Period, Power Level, Count Rate (12)
- SRNM Upscale/Inop Trip, Reactor Period Trip Status
- SRNM Upscale Rod Block, Reactor Period Rod Block, Downscale Rod Block Status
- SRNM Channel Bypass Status
- SRNM Period Based Permissive
- SRNM ATWS Permissive Status
- LPRM Bypass Status, LPRM Upscale Alarm, LPRM Downscale Alarm Status (256)

Number Bypassed LPRMs in APRM Channel:

- APRM Power Level (4)
- APRM Bypass Status (4)
- APRM Divisional Reactor Upscale/Inop Trip, Upscale Rod Block, Downscale Rod Block Status

- APRM Simulated Thermal Power Level (4)
- APRM Simulated Thermal Power Upscale Trip Status
- APRM ATWS Permissive Status (4)
- OPRM Divisional Trip Status
- MRBM Main Channel Bypass Status
- MRBM Main Channel Rod Block Status
- AFIP System Operability Status

The required alarms in the MCR include the following as a minimum:

- SRNM Upscale Trip, Upscale Rod Block
- SRNM Non-coincident Upscale Trip
- SRNM Non-coincident Upscale Rod Block
- SRNM Downscale Rod Block
- SRNM Short Period Trip, Short Period Rod Block
- SRNM Inoperative Trip
- SRNM Period Withdrawal Permissive Alarm
- LPRM Upscale, Downscale Alarm
- APRM Upscale Trip
- APRM Upscale Rod Block, Downscale Rod Block
- APRM Simulated Thermal Power Upscale Trip
- APRM Simulated Thermal Power Rod Block
- APRM System Inoperative Trip
- MRBM Upscale Rod Block, Downscale, Inoperative Rod Block
- AFIP Inoperative
- OPRM Trip

The above NMS displays and alarms satisfy the information display requirements of the IEEE Std. 603.

7.2.2.5.2 Basic Control Logic Requirements

The control logic of the safety-related subsystems in the NMS is designed as "fail-safe." That is, a trip signal is initiated if the control logic device fails because of critical hardware failure, power failure, or loss of communication failure.

The minimum required NMS controls located in the main control room panel include:

(1) SRNM Channel Bypass Controls (one for each bypass group) (hardware);

(2) APRM Channel Bypass Control (one for each division) (hardware); and

(3) Coincidence/Non-Coincidence switch. In the Non-Coincidence position (not in RUN mode), any single SRNM channel trip condition will send a trip signal to RPS and cause the reactor scram.

7.2.2.5.3 Basic Instrument Arrangement Requirements

NMS instruments and equipments are located in appropriate areas in the control building and reactor building, with appropriate divisional physical and electrical separation. Any NMS instruments located in the reactor building are in clean areas.

7.2.3 Suppression Pool Temperature Monitoring

The Suppression Pool Temperature Monitoring (SPTM) function, which is a subsystem of the Containment Monitoring System (CMS), is classified as safety-related because it can control nuclear safety-related systems or equipment.

7.2.3.1 Design Bases

Safety-Related Design Bases

The safety-related functional requirement of the SPTM is to prevent the suppression pool (S/P) temperature from exceeding the established limits. It does this by providing the inputs necessary for automatic scram initiation, which then serves to limit the heat addition to the suppression pool.

The SPTM is a safety-related four-divisional subsystem, Seismic Category I. The specific regulatory requirements applicable to this system are listed in Table 7.1-1 and individually addressed in Subsection 7.2.3.3.2.

Nonsafety-related Design Bases

The nonsafety-related functional requirements are:

- To provide input for automatic suppression pool cooling mode initiation; and
- To provide input for data display, alarm and recording on main control room panels.

7.2.3.2 System Description

General

The SPTM provides the suppression pool temperature data for automatic scram and automatic suppression pool cooling initiation, when established limits of high temperature are exceeded. The SPTM subsystem also provides S/P temperature data for operator information and recording and temperature information on post-accident conditions of the suppression pool. The SPTM subsystem outputs to other systems are shown in Table 7.2-4.

Power Sources

The suppression pool temperature monitoring hardware is redundantly powered by the appropriate divisional uninterruptible AC and interruptible ICP power sources, either of which can support the SPTM function.

Equipment Design

The suppression pool temperature monitoring system is composed of four independent instrumentation divisions. Each safety-related division contains sixteen thermocouples spatially distributed around the suppression pool. The sensor locations are established based upon the following considerations:

- Provide four-divisional, redundant measurement of S/P local and bulk-mean temperature, under normal plant operating conditions and under postulated accident and post-accident conditions;
- Implementing the divisional separation of sensors in the azimuthal directions, with redundancy and separation of sensors realized in four divisions, and with sensors appropriately covering the different elevations of the pool; and
- Locating sensors away from jet paths of SRV quenchers, horizontal vent discharges, and PCCS vent line discharges. This limits the maximum measurement differences between local and bulk-mean values.

The sensor electrical wiring, encapsulated in bendable, grounded sheathing, is terminated in the wetwell-sealed, moisture-proof junction box for easy sensor replacement or maintenance during the plant outage time. The thermocouple sensor wiring from the wetwell junction boxes is directed through the suppression pool divisional instrument penetrations to the four-divisional Essential Distributed Control and Information System (E-DCIS).

Signal Processing

Suppression pool temperature monitoring supports measurement and calculation of bulk average suppression pool temperatures for both normal operation and accident conditions. A minimum number of thermocouples per division are required to be operational and the SPTM logic will automatically compensate for inoperable thermocouples. If less than the required number of thermocouples is available, a trip signal will be generated in that division. These signals are transmitted, via divisional E-DCIS, to RPS. Safety-related protective actions are generated by the RPS. Abnormal status alarms, data display and recording are provided.

7.2.3.3 Safety Evaluation

7.2.3.3.1 General Functional Requirements Conformance

Suppression pool temperature monitoring is designed to support the maintenance of suppression pool temperature by providing four-divisional inputs for automatic scram initiation and temperature status display.

S/P temperature monitoring also provides Class 1E inputs to the main control room for indication, provides input for nonsafety-related S/P automatic cooling mode initiation, and for display, alarm and recording.

7.2.3.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the Suppression Pool Temperature Monitoring function and the associated codes and standards applied in accordance with the Standard Review Plan (SRP) 7.2. The

following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50 and 52:

50.55a(a)(1), Quality Standards for Systems Important to Safety

Conformance: SPTM complies with this requirement.

50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE279 and RG 1.75. The SPTM portion of CMS consists of four divisions, which are redundantly designed so that failure of any single temperature elements will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

Conformance: SPTM demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi), ITAAC in Design Certification Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

52.47(a)(1)(vii), Interface Requirements

Conformance: Interface material is provided in Tier 1.

52.47(a)(2), Level of Detail

Conformance: The level of detail provided for the SPTM subsystem within the Tier 1 and Tier 2 documents conforms to this BTP.

52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

52.79(c), ITAAC in Combined License Applications

Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC):

In accordance with Table 7.1-1, the following GDC are addressed for the SPTM subsystem:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24, 25, and 29.
- Conformance: The SPTM subsystem complies with the GDC identified. GDC conformance is generically discussed in Subsection 3.1.

Staff Requirements Memoranda:

Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs).

Conformance: The ESBWR SPTM subsystem and Engineered Safety Features (ESF) designs conform to the item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control, described in Section 7.8.

Regulatory Guides (RGs):

In accordance with Table 7.1-1, the following RGs are addressed for the SPTM subsystem:

RG 1.22 Periodic Testing of Protection System Actuation Function

RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System

RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Protection Systems

RG 1.62 Manual Initiation of Protective Actions

RG 1.75 Physical Independence of Electric Systems

RG 1.105 Setpoints for Safety-Related Instrumentation

RG 1.118 Periodic Testing of Electric Power and Protection Systems

RG 1.153 Power Instrumentation & Control Portions of Safety Systems

The SPTM subsystem conforms to all of the above listed RGs, with the same interpretations and clarifications identified in Subsection 7.2.1.3 also being applied to SPTM.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control (SSLC) Subsection 7.1.2.2.

Branch Technical Positions (BTPs):

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-1, the following BTP is addressed for SPTM:

HICB-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service

HICB-8 – Guidance for Application of RG 1.22

HICB-11 – Guidance on Application and Qualification of Isolation Devices

HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

HICB-17 – Guidance on Self-Test and Surveillance Test Provisions

HICB-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

HICB-19 – Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

HICB-21 – Guidance on Digital Computer Real-Time Performance

Conformance: The SPTM complies with all the above HICBs. Discussion of HICBs 14, 17, 18, 19 and 21 are addressed in conjunction with the Safety System Logic and Control System (SSLC) in Subsection 7.3.4.3 and with the RPS in Subsection 7.2.1.3.

TMI Action Plan Requirements:

In accordance with the SRP for 7.2 and with Table 7.1-1, only I.D.3 applies to the SPTM subsystem. This is addressed above for 10 CFR 50.34(f)(2)(v). However, TMI action plan requirements are generically addressed in Appendix 1A.

7.2.3.4 Testing and Inspection Requirements

Proper functioning of analog temperature sensors is verified by channel cross-comparison during plant normal operation mode; the bulk pool temperatures are continuously compared between divisions and alarmed for inconsistency by the plant computer functions.

Each of four suppression pool temperature monitoring safety-related divisions is testable during plant normal operation to determine the operational availability of the system. Each safety-related division of S/P temperature monitoring has the capability for testing, adjustment, and inspection during plant outage.

7.2.3.5 Instrumentation Requirements

The instrumentation and control requirements related to S/P temperature monitoring are addressed in Subsections 7.2.3.1 and 7.2.3.2.

7.2.4 COL Information

None.

7.2.5 References

7.2-1 GE Nuclear Energy, “General Electric Instrument Setpoint Methodology,” Licensing Topical Report NEDC-31336P-A, Class III (GE proprietary), September 1996.

Table 7.2-1

Channels Utilized in Functional Performance of RPS

Channel Description	Number of Channels of Sensors
Neutron Monitoring System (APRM)	4
Neutron Monitoring System (SRNM) (Note 1)	4 (12 sensors)
Nuclear system reactor vessel pressure	4
Drywell pressure	4
Reactor vessel narrow range water level	4
Low charging pressure to rod hydraulic control unit accumulator	4
MSL isolation valve position switches	8
TSV closure	4
TCV fast closure	4
Loss of Power Generation Bus (Loss of FW Flow)	4
High Condenser Pressure	4
Suppression pool temperature monitoring	4

1. In modes other than RUN

Table 7.2-2

SRNM Trip Function Summary

Trip function	Typical Analytical Limit For Trip Setpoint (Note 1)	Action
SRNM Upscale Flux Trip	45% power (Note 2)	Scram (bypassed in RUN)
SRNM Upscale Flux Alarm	35% power (Note 3)	Rod Block (bypassed in RUN)
SRNM Short Period Trip	10 second	Scram (Note 4) (bypassed in RUN & REFUEL) (no scram function in counting range)
SRNM Short Period Alarm	20 second	Rod Block (bypassed in RUN)
SRNM Period Control Rod Withdrawal Permissive	55 second	Rod Block (bypassed in RUN) (Note 5)
SRNM Inoperable	Module interlock disconnect; HV voltage low	Scram (bypassed in RUN)
SRNM Downscale	3 cps	Rod Block
SRNM Intermediate Upscale Flux Trip	5E+5 cps	Scram (Note 6)
SRNM Intermediate Upscale Flux Alarm	1E+5 cps	Rod Block (Note 6)
SRNM ATWS Permissive	6% power	Permissive signal to SLC system (all modes)

Notes:

1. Values in this table are typical. Instrument accuracy will be considered in the setpoint methodology (Reference 7.2-1).
2. This scram setpoint is equivalent to the upscale scram on the last range of BWR/5 IRM, at the 120/125 level.
3. This rod block setpoint is equivalent to the upscale rod block on the last range of BWR/5 IRM, at the 108/125 level.
4. Scram action only active in mean square voltage range, which is defined as above $1x10^{-4}$% power.
5. With the rod block at this setpoint, the reactor period never reaches 10 seconds because of rod withdrawal. Consequently, no reactor scram would result.
6. In NMS NON-COINCIDENCE mode. Conditions for activation will be defined in the plant operating procedures.

Table 7.2-3

APRM Trip Function Summary

Trip Function	**Typical Analytical Limit For Trip Setpoint** (Note 1)	**Action**
APRM Upscale Flux Trip	120% power 15% power	Scram (only in RUN) Scram (not in RUN)
APRM Upscale Flux Alarm	108% 12% power	Rod Block (only in RUN) Rod Block (not in RUN)
APRM Upscale Simulated Thermal Power Trip	115%	Scram
APRM Inoperative	1. LPRM input too few; 2. Module interlocks disconnect	Scram & Rod Block Scram & Rod Block
APRM Downscale	5%	Rod Block (only in RUN)

1. Values in this table are typical. Instrument accuracy will be considered based on the instrument setpoint methodology of Reference 7.2-1.

Table 7.2-4

Outputs from SPTMs to Other Systems

Signal	Utilization
Sixteen divisional S/P local temperature signals to each Essential DCIS RMU (in each of 4 divisions).	Input for divisional scram initiation and temperature status display within SSLC and RPS. Input for non-divisional S/P cooling mode initiation (FAPCS). Input for non-divisional S/P temperature data display, alarm and recording (within NE-DCIS & MCR).

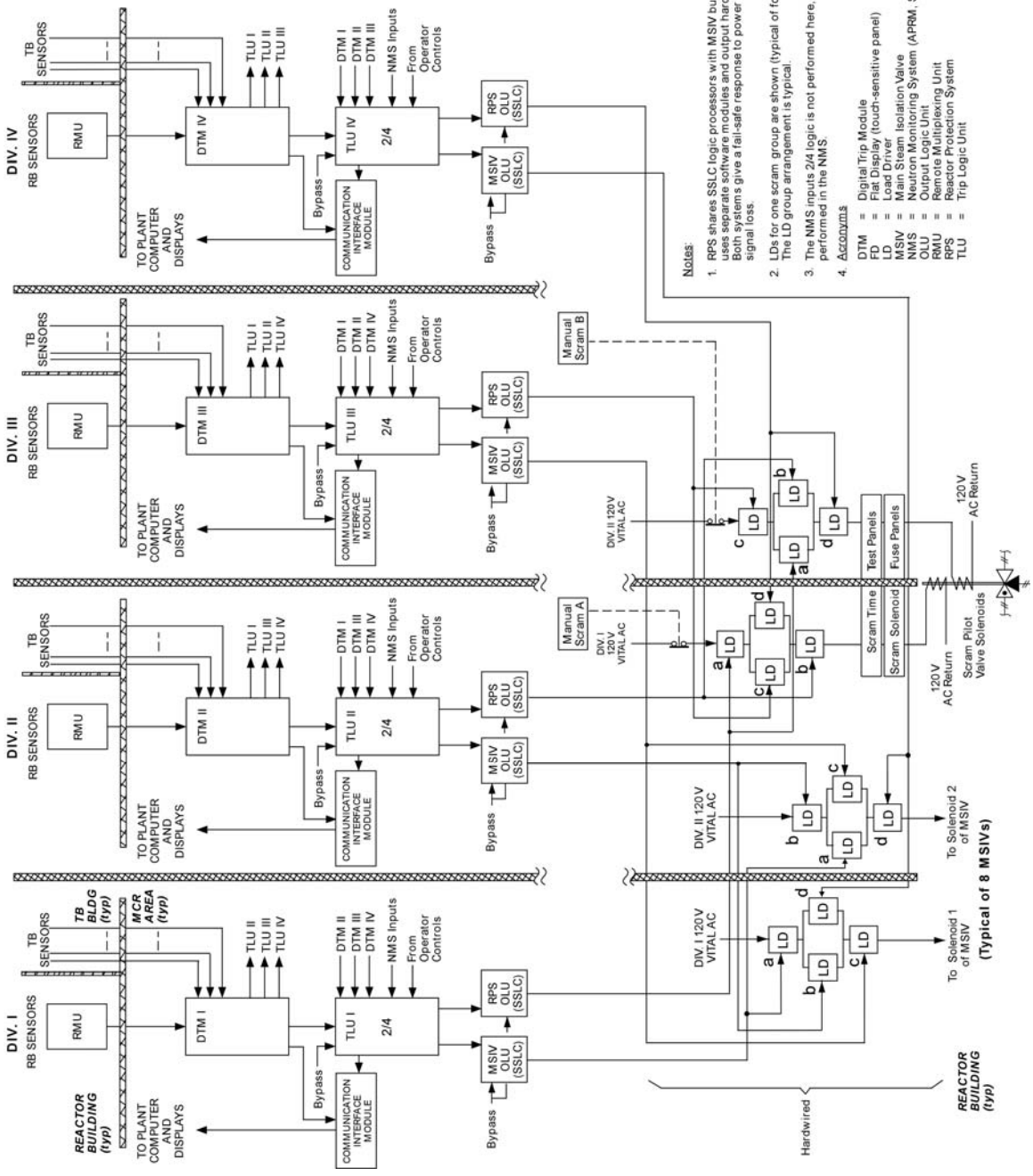


Figure 7.2-1. RPS Functional Block

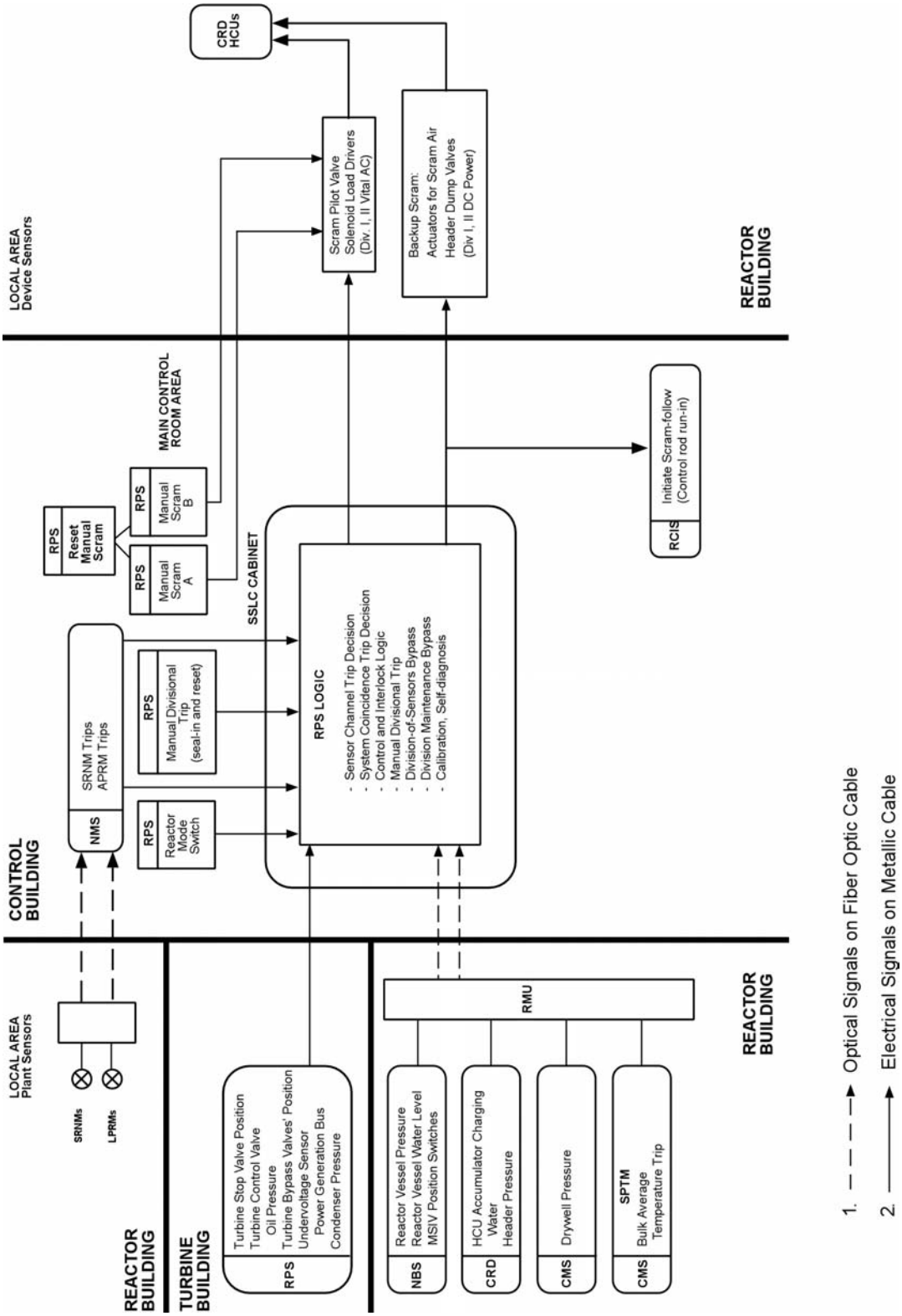


Figure 7.2-2. RPS Interfaces and Boundaries Diagram

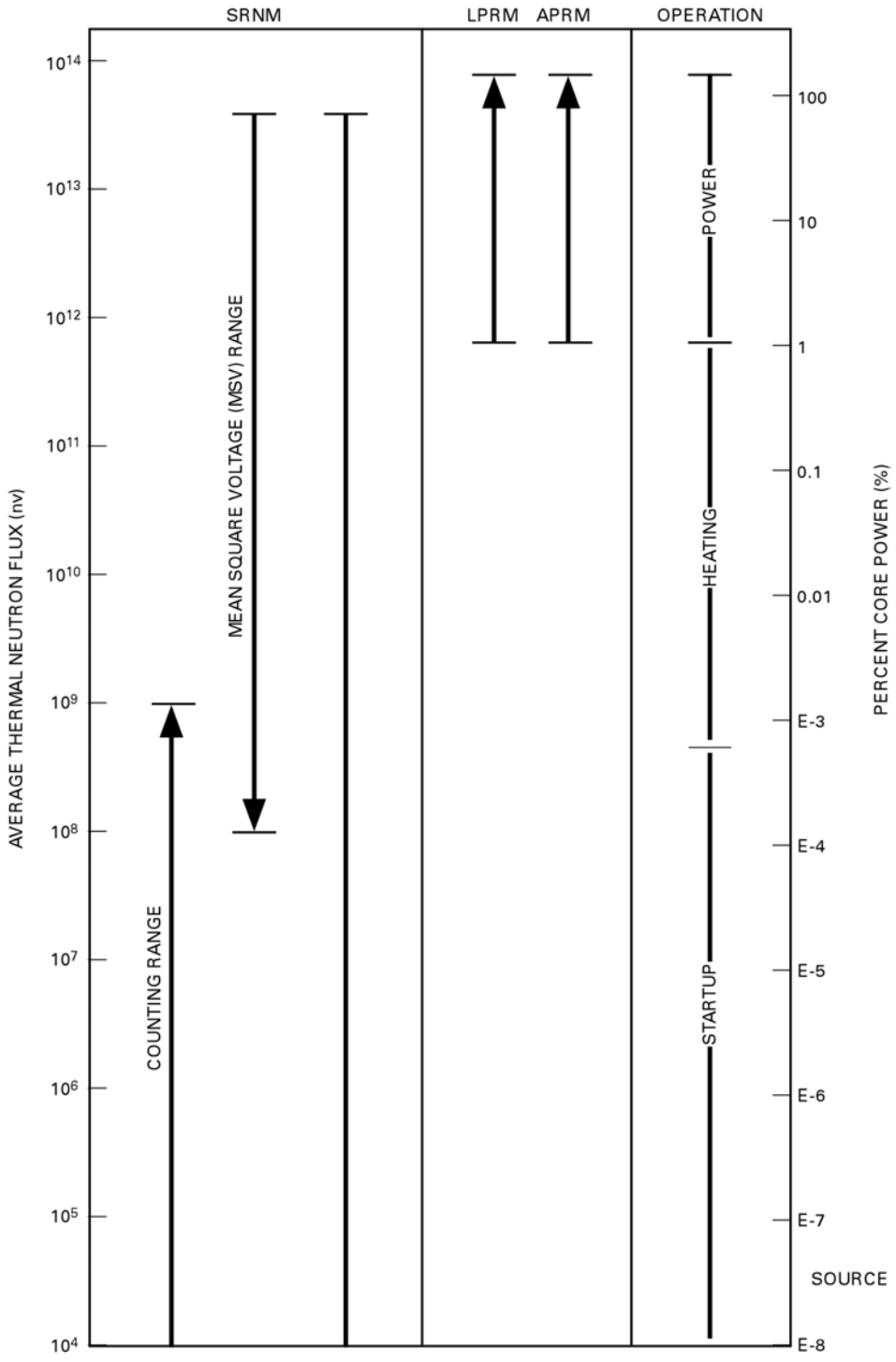


Figure 7.2-3. Neutron Flux Monitoring Ranges

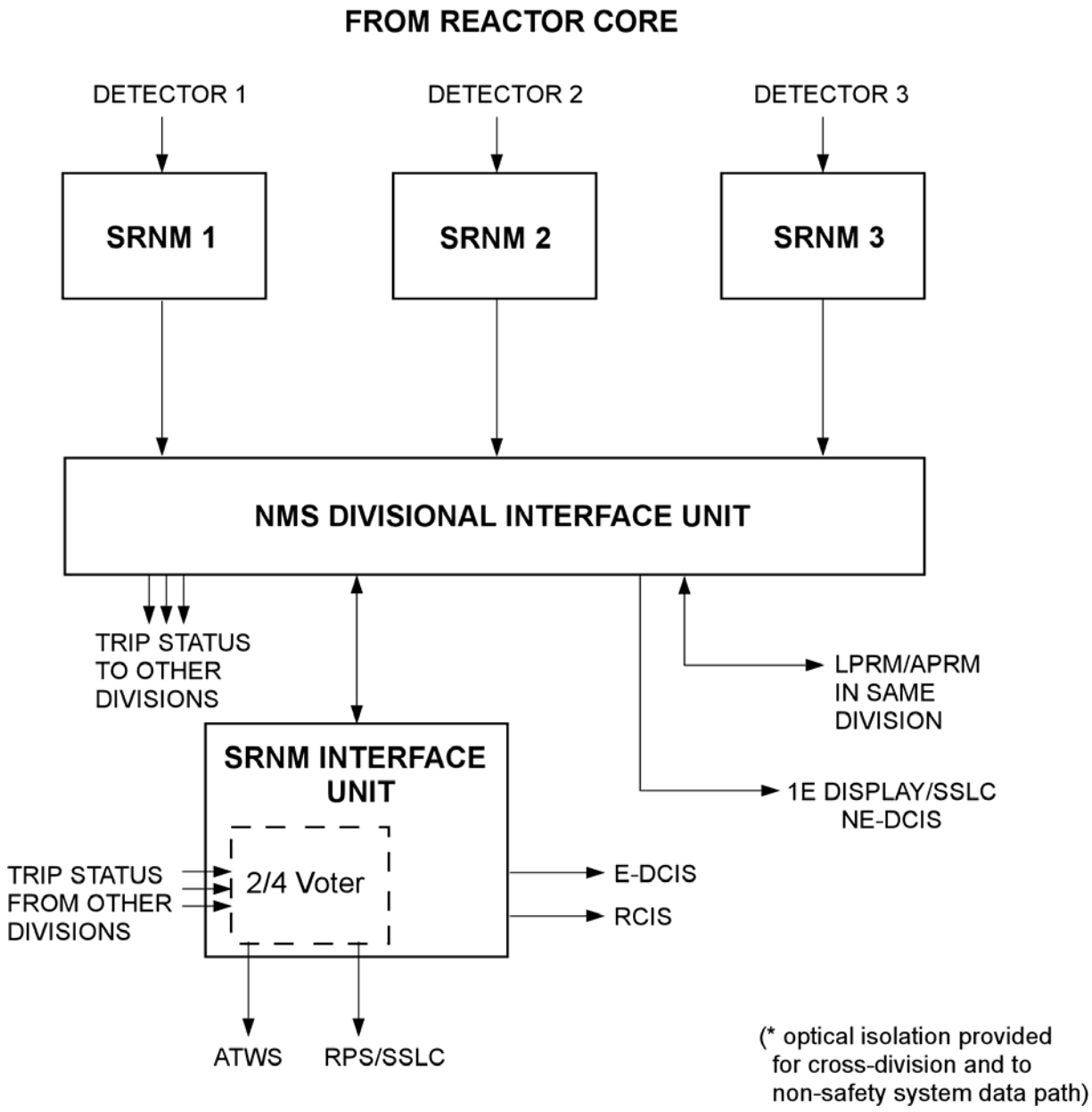


Figure 7.2-4. Basic Configuration of a Typical SRNM Subsystem

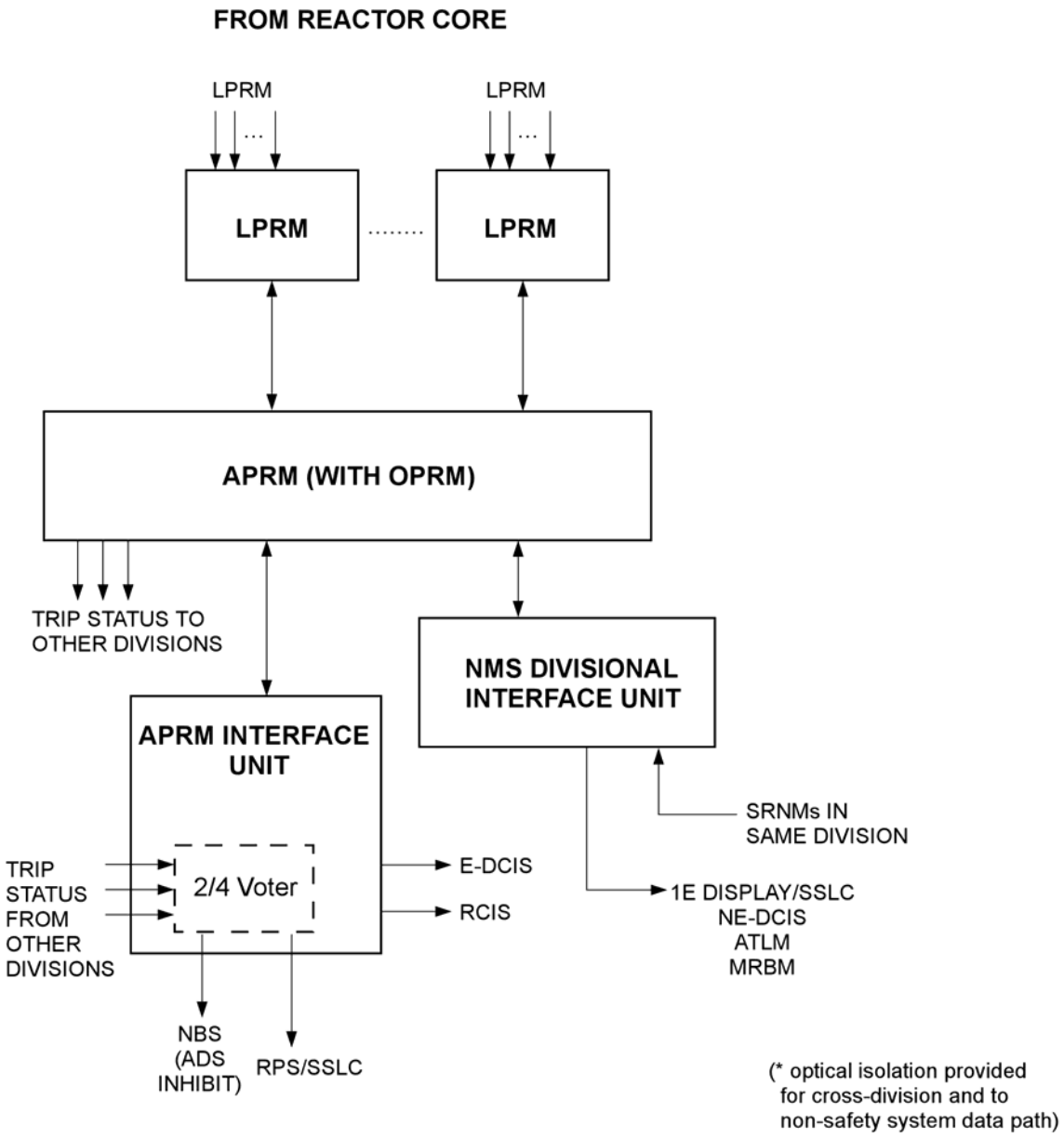


Figure 7.2-5. Basic Configuration of a Typical PRNM Subsystem

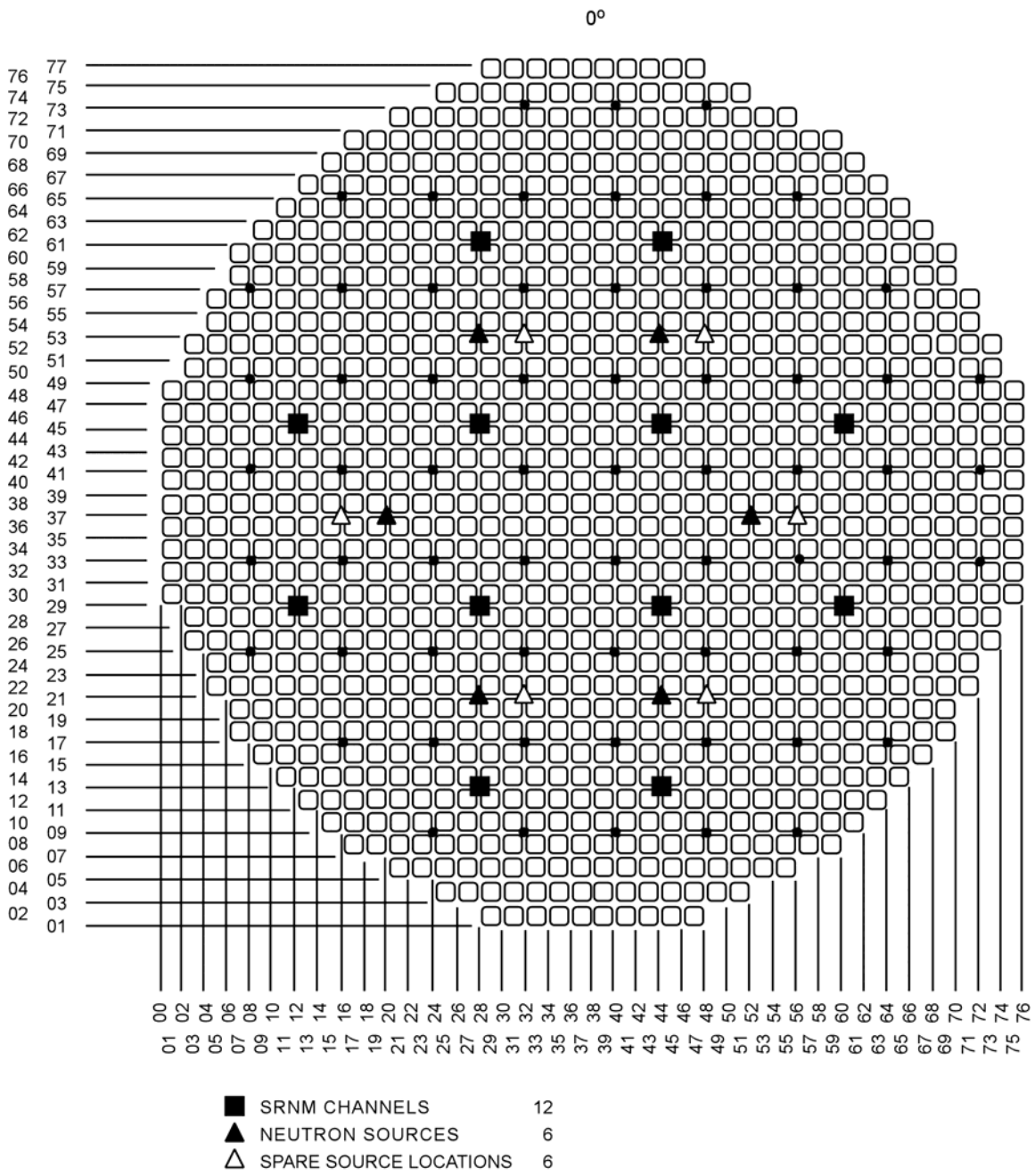


Figure 7.2-6. SRNM Detector Locations

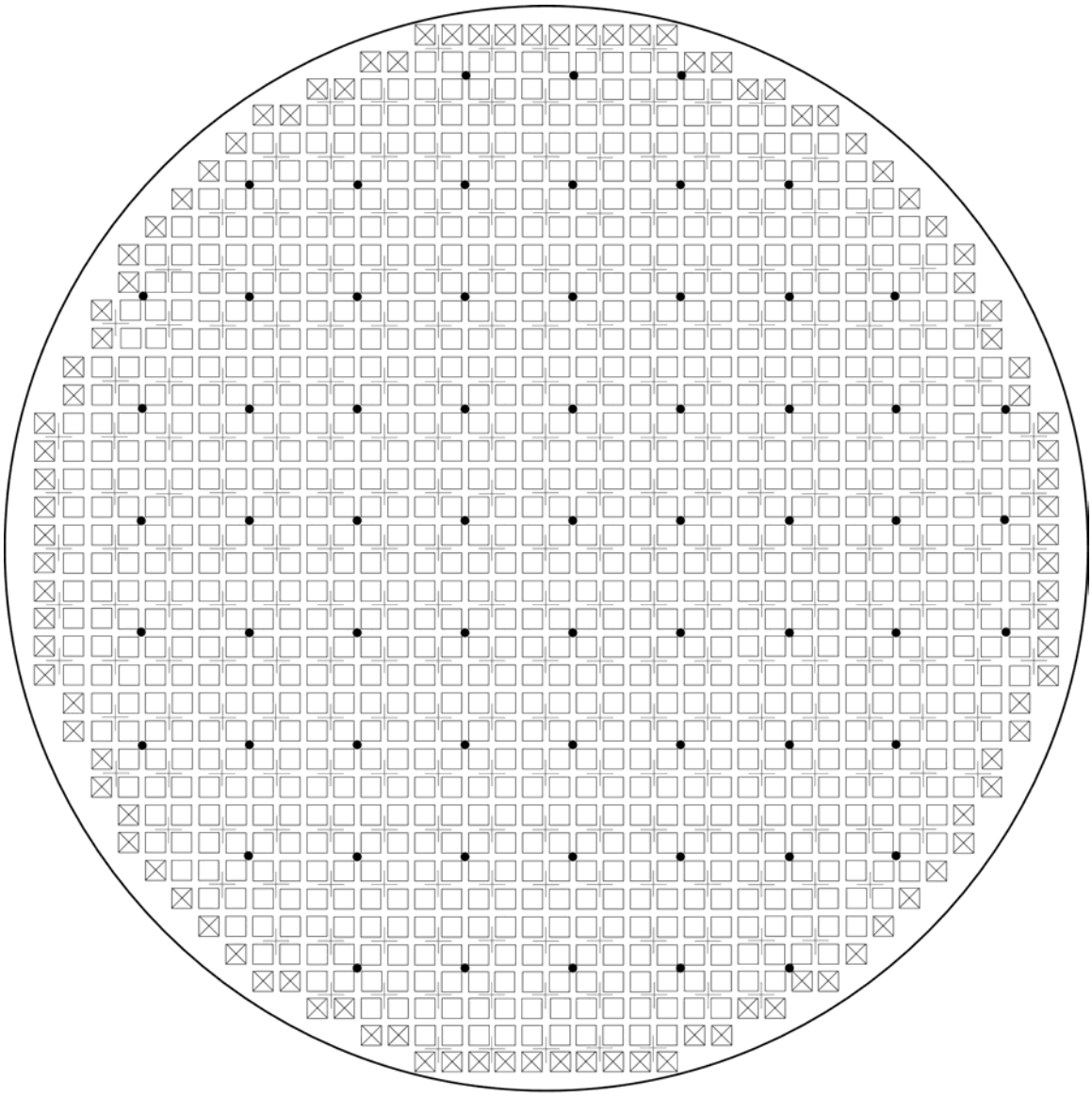


Figure 7.2-7. LPRM Locations in the Core

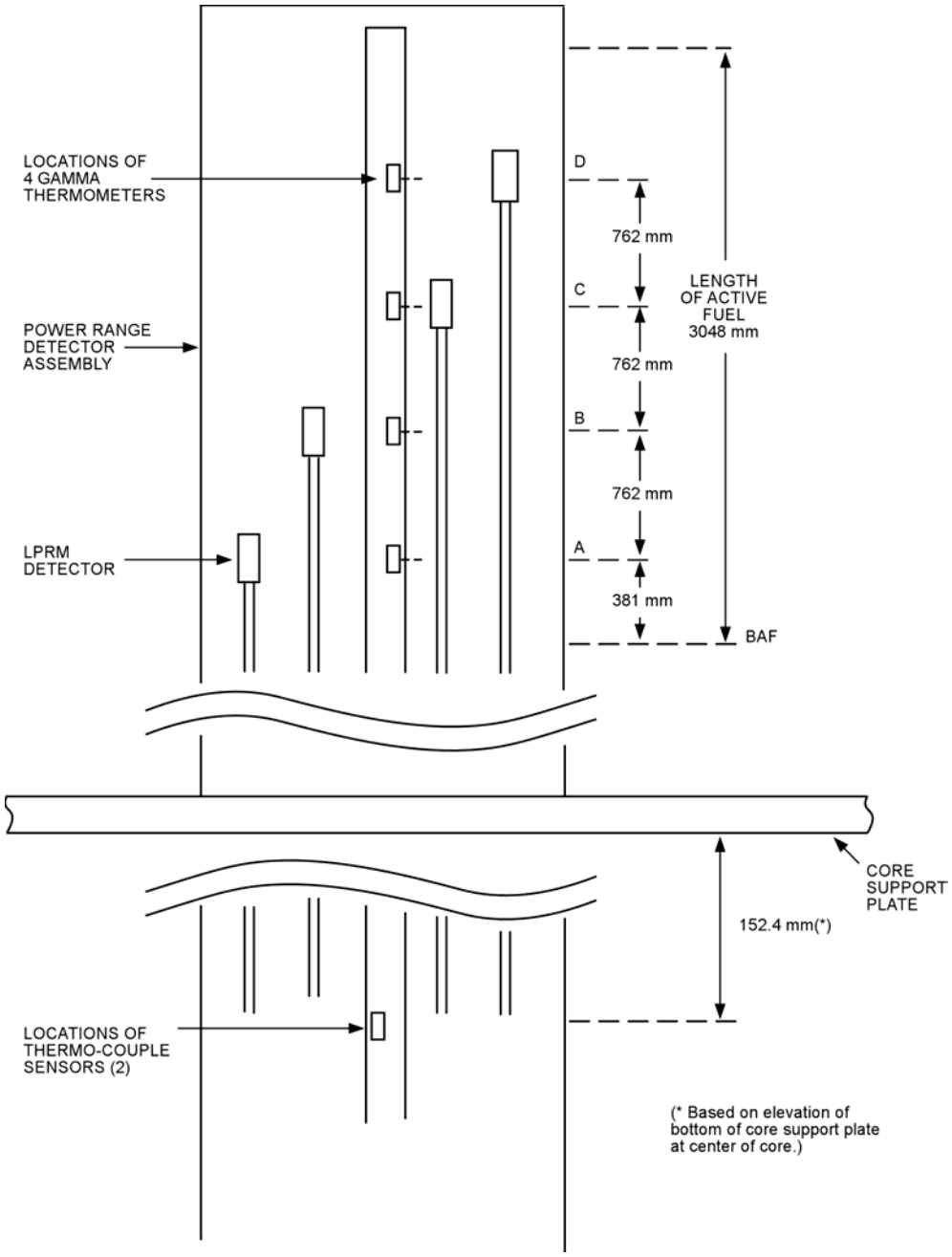


Figure 7.2-8. Axial Distribution of LPRM Detectors

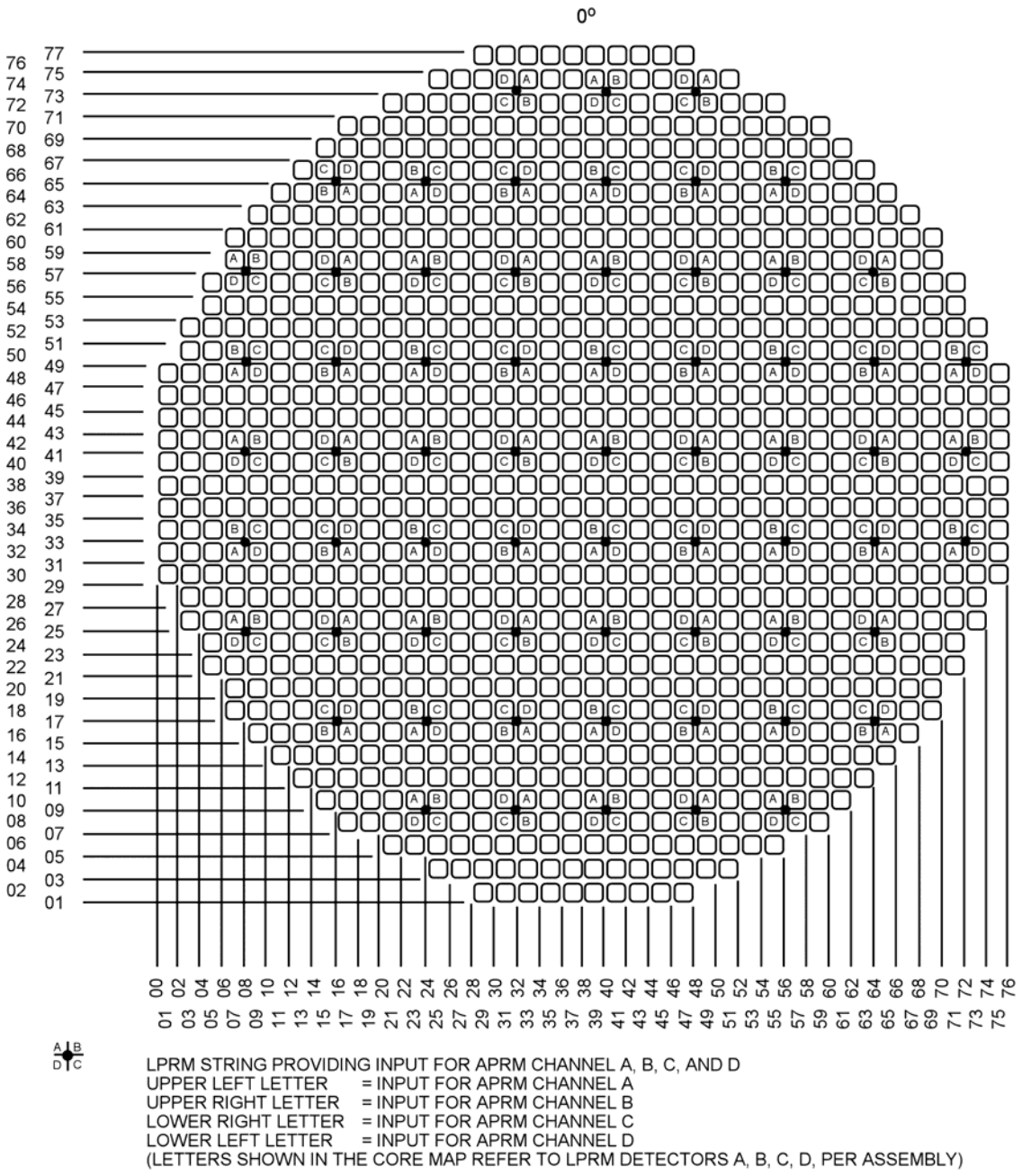


Figure 7.2-9. LPRM Assignments to APRM Channels

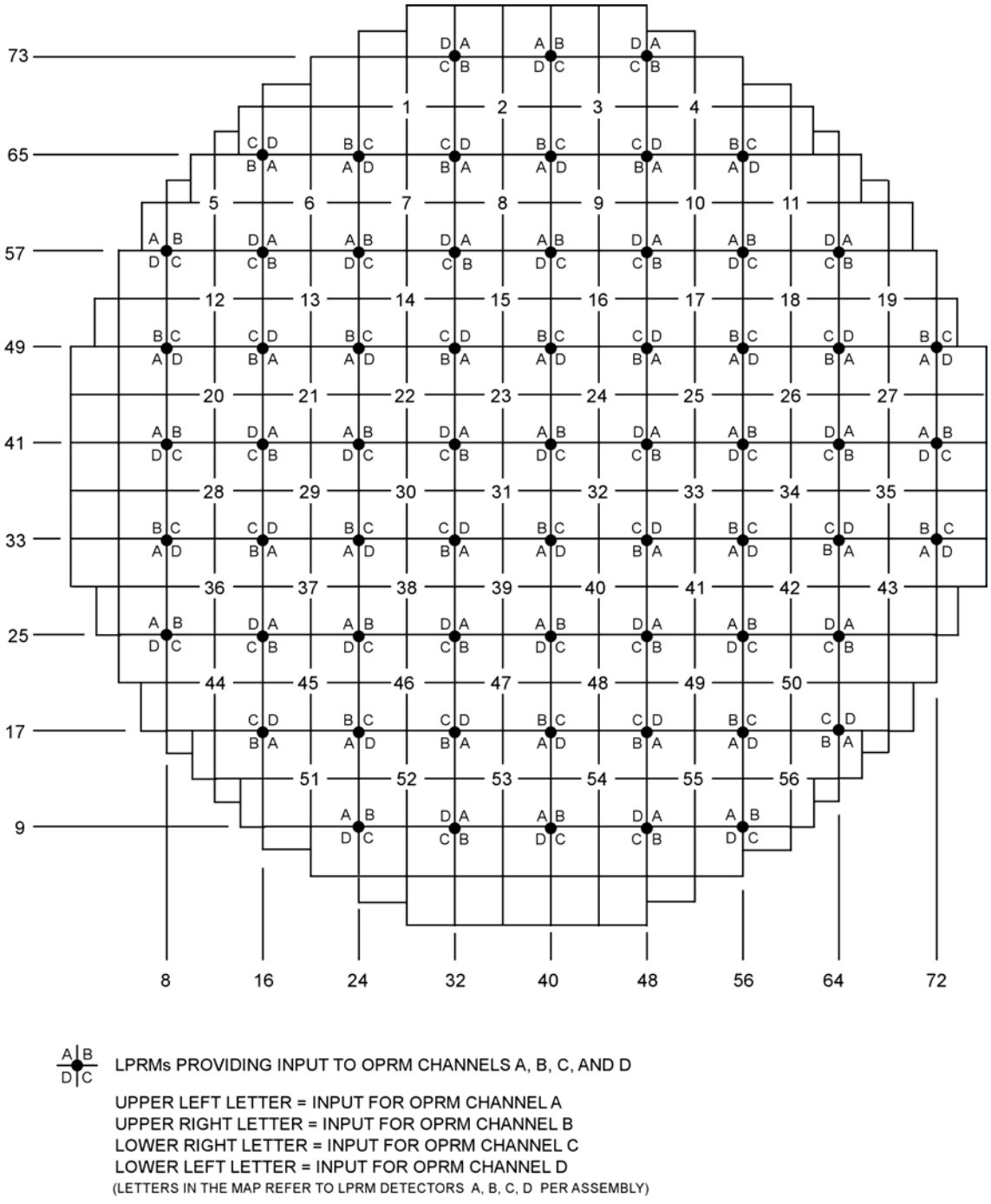


Figure 7.2-10. LPRM Assignment to OPRM Channels

7.3 ENGINEERED SAFETY FEATURES SYSTEMS

7.3.1 Emergency Core Cooling System

7.3.1.1 Automatic Depressurization System (ADS) Function

7.3.1.1.1 Design Basis

Safety (10 CFR 50.2) Design Bases

The ADS controls and instrumentation shall meet the following safety-related requirements:

- Detect reactor low water levels Level 1.5 and Level 1;
- Detect containment drywell high pressure;
- Automatically actuate the safety/relief valves (SRVs) and depressurization valves (DPVs) after Level 1.5 is reached in conjunction with high drywell pressure or after vessel level remains at or below Level 1.5 for a prescribed time. Additionally, the SRVs and DPVs will be actuated after Level 1 is reached;
- Actuate the SRVs and DPVs sequentially and in groups to achieve the required depressurization characteristics;
- Any single failure shall not render more than one valve inoperative; and
- Have physical and electrical separation and isolation between safety-related divisions and from nonsafety-related circuits and equipment.

Nonsafety Design Basis

The ADS instrumentation shall meet the following nonsafety-related requirements:

- No single control or instrumentation failure shall inadvertently open an SRV or a DPV
- Indicate status of SRVs and DPVs in the main control room; and
- ADS-parameters alarm provided in the main control room.

7.3.1.1.2 System Description

Summary Description

The ADS is part of the Emergency Core Cooling System (ECCS) and resides within the Nuclear Boiler System (NBS). It depressurizes the reactor so the low-pressure Gravity-Driven Cooling System (GDCS) can provide make up coolant to the reactor. The ADS comprises the SRVs and DPVs and associated instrumentation and controls. Five SRVs are initially opened to start reducing reactor pressure vessel (RPV) pressure, followed by five more SRVs after a time delay. The sequence continues with groups of DPVs each opening after further successive time delays. This sequential operation minimizes the amount of water lost as a result of level swell in the reactor pressure vessel (RPV) when the RPV pressure is rapidly reduced.

The NBS function components (including the ADS) are shown on Figure 5.1-2. The mechanical aspects of the ADS function within the ECCS are discussed in Subsection 6.3.3 and the ADS logic and control are shown on Figures 7.3-1A and 7.3-1B.

System Design

The ADS design parameters shown in Table 7.3-1 ensure that no single failure of an ADS division logic, SRV actuation pilot or DPV igniter circuit can prevent successful system operation. This satisfies the single failure criterion of IEEE Std. 603.

ADS Input Circuits

Actuation of ADS equipment is performed automatically, without need for operator action. Manual actuation is also possible.

Four wide range reactor level transmitters are used to detect both Level 1.5 and Level 1; these transmitters are separate from those used for RPS functions and diverse to those used for the DPS wide range level transmitters.

Four pressure transmitters are used to detect drywell pressure; these transmitters are diverse from both the DPS and RPS drywell pressure transmitters.

Logic and Sequencing

The ADS logic is implemented in four divisions, each of which can make a Level 1.5, Level 1 and high drywell pressure trip decision. Analogous to RPS, each of the trip decisions is shared between the four divisions. Normally each of the four divisions will make a 2 out of 4 trip decisions from each of the four divisional trip decisions, however the entire ECCS system has a "division of sensors" joystick bypass switch such that any division's sensors can be removed from the 2 out of 4 decision process. The bypass is enforced by the switch to allow only one division at a time to be bypassed and can be used for maintenance or calibration activities. The use of the sensor bypass switch does not affect any division's ability to make 2 out of 4 trip decisions such that no ECCS protection is lost by the use of the bypass. Divisional bypasses are alarmed in the main control room and the four divisional water levels and drywell pressures and their trip setpoints are continuously monitored and alarmed for consistency by the NE-DCIS plant computer functions.

Unlike the RPS design, each division of the ECCS has two channels of 2-out-of-4 trip logic to support the requirement that single divisional failures do not inadvertently open any ADS (SRV or DPV) valve. Each division's initiating logic (DTM) now has access to one channel of separate Level 1.5, Level 1 and high drywell pressure trip decisions (before the VLU). The separate logic of the channel will start a timer on reaching Level 1.5 and monitor the high drywell pressure decision. If high drywell pressure exists OR the timer times out, an ECCS trip signal will be issued. The timer will automatically reset if reactor level increases above Level 1.5 and restart if level again drops below Level 1.5.

Additionally the channel logic will each issue the ECCS trip signal if level drops below Level 1.

The ECCS trip signal then starts a nominal 10 second timer; should the trip signal reset (as, for example, from an instrument column transient), the timer will reset and restart when the next ECCS trip signal is received. If the ECCS trip signal persists for a nominal ten seconds, the logic will seal in and issue an "initial start" signal. The initial start signal is also sent to the SLC system, IC and GDCS logic discussed later. The initial start signal specifically initiates five timers in each of the two 2-out-of-4 trip logic channels (per division) of ADS logic.

These five timers apply to the time delays of six sets of valve openings, i.e., initial start (no delay) for Group 1 of 5 SRVs, and subsequent delays for Group 2 of 5 other SRVs, Group 1 of 3 DPVs, Group 2 and 3 for each of 2 DPVs and Group 4 of 1 DPV. As such, there is an initial ADS start signal (per channel), and then a time delayed second (per channel), third (per channel), fourth (per channel), fifth (per channel) and sixth (per channel) ADS start signal. The definitions of these ADS group assignments are described in Table 7.3-2 and Table 7.3-3, where the DPVs' number of assigned groups, number of valves per group, and group initiation signal time delays are explained. Once the initial start signal is generated the timers cannot be reset and all six starting signals (per channel) will be issued.

The first (initial) start signal will open five SRVs to initially reduce reactor pressure; the second start signal will open the remaining five SRVs. The third start signal will open three of the DPVs (this signal is also made available to ATWS/SLC system discussed later) and the fourth through sixth start signals will open the remaining DPVs in groups of two, except Group 4 which is one DPV. This sequential operation facilitates rapid depressurization while minimizing the amount of water lost as a result of level swell in the reactor that occurs when pressure is rapidly reduced.

The two channels of ADS start signals (initial through sixth within a division) are sent to the load drivers for the SRVs and DPVs operated by that division. The load drivers are wired in series for each valve such that both are required for operation; this scheme makes the logic single failure proof against inadvertent actuation. Each SRV and each DPV is connected to two divisions of power (two divisional solenoids for SRVs and two squib initiators for the DPVs) with the solenoids and initiators evenly spread among the four divisions and never the same division on any one valve. The logic is such that either division will open the SRV/DPV; this makes the design single failure proof against not opening every valve.

Divisional separation is maintained through the use of optical isolators and separated raceway, conduit, penetration wiring to each SRV or DPV. Any three divisions can open all of the valves.

Additionally, as discussed in Subsection 7.8.1.2, the Diverse Protection System (DPS) also has the ability to independently open the same SRVs and DPVs using the same logic but using a completely diverse hardware/software equipment and separate reactor level and drywell pressure sensors used in the primary ECCS functions. In the case of the SRVs the DPS uses a third, nonsafety solenoid on each of the SRVs.

The SRVs are described in detail in Subsection 5.2.2 and the DPVs are described in detail in Subsection 6.3.3.

A control switch is furnished in the main control room for each of the SRVs that allows the operator to manually open each valve independently (using the primary SRV logic function). Besides, any nonsafety VDU in the main control room will be able to provide a display format, which will allow the operator to individually open an SRV independently using the DPS function. These two manual opening schemes are completely diverse from one another.

Two control switches on the Division I MCR panels are furnished to allow the operator to manually open the four DPV valves connected to Division I independently by injecting manual trip signals into the DPV automatic logic. These switches will be of the "arm/fire" type and wired in series such that four deliberate operator actions (two for "arm" and two for "fire") are required to operate the DPVs. A similar arrangement is provided for the one half of the DPVs

operated by Division II. Any nonsafety VDU in the main control room will be able to provide a display format that will allow the operator to individually open each DPV independently of the DPS automatic logic. These display formats will require at least three deliberate operator actions per DPV. The two manual opening schemes from the primary ECCS and from DPS are completely diverse from one another.

Finally four "arm/fire" switches (one per division) are furnished to manually initiate ADS as a system instead of each valve individually. If the operator uses any two of the four switches, the ADS sequence will seal in and start the ADS valve sequencing. This requires four deliberate operator actions. For all of the manual initiations, operator use of the "arm" portion of the switch or display will cause a plant alarm.

See Figure 7.3-1A for a typical SRV actuation logic and Figure 7.3-1B for a typical DPV actuation logic.

The actual firing circuit for the various squib initiators and SRV solenoids is a series circuit of the two load drivers followed by a continuity monitor and then a keylock switch, all located in the appropriate divisional remote multiplexing units and DPS remote multiplexing unit in the reactor building. Because there is the division of sensor bypass, and there are two channels of 2-out-of-4 logic, no additional division of trip logic bypass is implemented in the ECCS logic. It is undesirable to perform this level of bypass activities with the RMU electrically connected to the valve. The keylock switch described below provides effective bypass function required. In addition to the usual RMU self diagnostics, means are provided to indicate that each of the series load driver circuits can be "closed" (these can be exercised one at a time from the control room) and to indicate that both have closed.

The keylock switch (shown in Figure 7.3-1A and Figure 7.3-1B) that disables the firing circuit is per valve and does not interact with the other valves on that RMU; operation of any keylock switch will cause a control room alarm to indicate that the firing circuit is out of service. Although the load driver checks can be done online (one at a time) without causing valve operation, opening the firing circuit with the keylock switch allows the continuity monitor to be tested and additionally allows on line surveillance and maintenance activities to be done, with the assurance that the valve will not be opened inadvertently. The operation of a keylock switch in any one division does not disable the SRV or DPV since it may still be opened by it's other divisional solenoid/squib initiator. Additionally it is not possible to lose the single failure inadvertent actuation protection by any operator or keylock switch action.

Supporting Systems

Supporting systems for the ADS include the instrumentation, logic, control and motive power sources. The instrumentation and logic power is obtained from corresponding divisional uninterruptible and ICP 120 VAC power sources; either source can support ADS operation. The actual SRV solenoid and DPV squib initiator power is supplied by the corresponding divisional 250 VDC batteries. The motive power for the electrically operated pneumatic pilot solenoid valves on the SRVs is from accumulators located near the SRVs, which are supplied with nitrogen by the High Pressure Nitrogen Supply System.

7.3.1.1.3 Safety Evaluation

Chapter 15 and Section 6.3 evaluate the individual and combined capabilities of the ECCS systems, including ADS. For the entire range of nuclear process system break sizes, the ECCS systems ensure that the reactor core is always covered.

ECCS initiating instrumentation, including the ADS, must respond to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant pressure boundary. Because reactor vessel low water level and drywell pressure parameters are the only ones completely independent of breach location, they are used to initiate ADS.

The redundancy of the control and monitoring equipment for the ADS is consistent with the redundancy of the four divisions of ADS.

No single failure in the ADS initiation circuitry can prevent the ADS from depressurizing the RPV, or cause an inadvertent actuation of ADS. This satisfies the single failure criterion of IEEE Std. 603.

The ADS has no equipment protective interlocks that could interrupt automatic system operation.

The ADS instrumentation, logic, and the SRV and DPV initiation circuitry is powered by divisionally separated safety-related 120 VAC and 250 VDC power.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the ADS and the applicable codes and standards. These are discussed below:

10 CFR 50.55a(1) (Quality Standards for Systems Important to Safety)

Commitment to regulatory guides and standards, as addressed in this section, satisfies 10 CFR 50.55a(1).

10 CFR 50.55a(h) (IEEE 279)

Conformance: IEEE Std 603 supercedes IEEE Std 279. Addressing RG 1.153 and IEEE 603, as discussed in Subsections 7.1.2.3.3, 7.1.2.3.6, and 7.2.1.2.4 (including design criteria discussions on quality, system integrity, independence, etc.) satisfies 10 CFR 50.55a(h) and IEEE Std 603.

10 CFR 50.34 (f) (2) (v) (I.D.3)

Commitment to regulatory guides and standards, as addressed in this section, satisfies 10 CFR 50.34 (f) (2) (v) (I.D.3).

10 CFR 50.34 (f) (2) (xiv) (II.E.4.2)

Commitment to regulatory guides and standards, as addressed in this section, satisfies 10 CFR 50.34 (f) (2) (xiv) (II.E.4.2).

10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Resolution of unresolved and generic safety issues is discussed in Section 1.11

10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications

ITAAC are provided for I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii) Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.47(a)(2) Level of Detail

The level of detail provided for the NBS within the Tier 1 and Tier 2 documents conforms to this BTP.

10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria

In accordance with the SRP for Subsection 7.3 and Table 7.1-1, the following GDC are addressed for the ADS System:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23 and 24.
- Conformance: The ADS complies with these GDC.

SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems)

Conformance: In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this SRM, the ADS function and other Engineered Safety Features (ESF) designs conform with the Item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8.

Regulatory Guides (RGs)

RG 1.22 - Periodic Testing of Protection System Function - System logic is tested continually as described in Subsection 7.3.1.1.4. Components are tested periodically during refueling outages every two years. The ADS fully conforms to this RG with the clarification that for the DPVs, periodic testing is interpreted to mean testing of the squib initiators in a laboratory after removal from the squib valves.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - The ADS fully meets the guidance of RG 1.47. Automatic indication is provided in the control room to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Protection Systems - The ADS meets the requirements of RG 1.53 in addition to Section 5.1 of IEEE 603 and IEEE 379.

RG 1.62 - Manual Initiation of Protective Actions - The ADS fully conforms to this RG. Manual actuation of ADS requires the operator to actuate at least two dual action switches. This ensures that the manual initiation of ADS is a deliberate act.

RG 1.75 - Physical Independence of Electric Systems - Physical separation is maintained in accordance with RG 1.75 and is described in Subsection 7.3.1.1.2.

The redundant equipment and circuits within the ADS have divisional separation. Redundant circuits and equipment are located within their respective divisional safety class enclosures. Separation is achieved by barriers, isolation devices or physical distance; thus, assuring that a single failure in one division would not affect the operation of other redundant divisions.

No physical connections are made between divisions except through nonmetallic fiber-optic medium.

Non-Class 1E circuits are in accordance with Class 1E circuit requirements up to and including the isolation devices. Circuits beyond the isolation devices do not again become connected with Class 1E circuits.

Separation between Class 1E and non-Class 1E circuits either satisfies the same minimum requirements as that for the separation between Class 1E circuits or they are treated as associated circuits.

RG 1.105 - Instrument Setpoints for Safety Related Systems - The setpoints used to initiate ADS are established consistent with this guide. Because the discrete setpoints in the ADS logic do not drift, most of the variation is expected to be in the process transmitters. Setpoints are continuously monitored and alarmed by the plant computer functions. The GE design document titled "General Electric Instrument Setpoints Methodology", Reference 7.2-1, provides the detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The ADS conforms to the intent of RG 1.118 as amplified in IEEE 338. A full functional test of the ADS is not practical, because a loss-of-coolant event results if the non-reclosable DPVs are opened. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is periodically self-tested and initiating circuits are continuously monitored as described in Subsection 7.3.1.1.4.

DPV valve initiators are periodically removed and test fired in a laboratory. Reactor vessel level and drywell pressure transmitters are located outside containment and calibration verification can be performed during plant operation.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The ADS fully conforms to this regulatory guide.

Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are discussed in Subsection 7.1.2.2.

Branch Technical Positions (BTPs)

BTP HICB-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

This BTP is not applicable to the ESBWR, in that it has no reactor recirculation pump.

BTP HICB-6 – Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The ESBWR has no recirculation pump and has no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 – Guidance on Application of Regulatory Guide 1.22

This BTP calls for the identification of the actuated equipment that is not tested during reactor operation and a discussion of how each conforms to the justification criteria of Paragraph D.4 of RG 1.22.

Because the DPVs are squib-actuated and cannot be closed once they are opened, there is no practicable system design that would allow testing during reactor operation without creating an unacceptable breach of the reactor coolant pressure boundary. The SRVs may be tested with the reactor at low power and at, or near rated pressure. Both the squib wires and the SRV solenoids are continuously monitored for electrical continuity, as indicated in Subsection 7.3.1.1.4.

The SRVs and DPV initiators can be tested when the reactor is shut down.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices

ADS conforms to this BTP. ADS logic is controlled by the SSLC system. SSLC logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

BTP HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

The ADS conforms to this BTP. Additional discussion is in Subsection 7.2.1.3.

BTP HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 DFR Part 52.

This BTP is applicable to all sections of the DCD including this section on ADS. This section content conforms to this BTP.

BTP's HICB-14, HICB-17, HICB-18, HICB-19 and HICB-21 are discussed in association with the SSLC in Subsection 7.3.4.3.

7.3.1.1.4 Testing and Inspection Requirements

The ADS trip logic units continuously self-test, as shown in Table 7.3-1. A very low current is used to test the continuity of the SRV pilot solenoids and the bridge wires within the DPV squib valve actuating circuitry. The test current is continuously applied and results in an alarm if the circuit is interrupted. Testing of ADS equipment is conducted during refueling outages. Refer to Subsection 6.3.2.8.4 for a discussion of mechanical tests performed on the ADS. (The same continuity test is also applied to the GDCS squib valves described in Subsection 7.3.1.2.)

7.3.1.1.5 Instrumentation Requirements

System status during normal plant operation and ADS performance monitoring in an accident is based on the following control room indications:

- Status indication of the SRVs and DPVs;
- SRV discharge line temperature alarm;
- RPV pressure indication;

- Suppression pool high/low level alarm;
- GDCS pool low level alarm;
- Water level indication for the GDCS pools, suppression pools, and RPV
- Alarms for the following ADS parameters in the main control room:
  - Manual arming of ADS;
  - Manual actuation of ADS;
  - Two-out-of-four ADS level 1.5 and level 1 signals;
  - Two out of four high drywell pressure signals;
  - Automatic ADS initiation;
  - Aborted ADS initiation;
  - SRV solenoid loss of continuity;
  - DPV squib firing circuit loss of continuity;
  - Inconsistent wide range divisional water level alarms; and
  - Inconsistent divisional drywell pressure alarms.
  - Any inconsistency of divisional input information from the four SSLC/ESF divisions to each VLU, as compared at the VLUs.
  - Any single one load driver trip in a firing circuit of a DPV

ADS instrumentation located in the drywell that is essential for system operation is designed to operate in an environment resulting from a loss-of-coolant accident. Safety-related instruments located outside the containment are also qualified for the environment in which they must perform their safety function.

7.3.1.2 Gravity-Driven Cooling System

7.3.1.2.1 Design Bases

Safety (10 CFR 50.2) Design Bases

The Gravity-Driven Cooling System (GDCS) control and instrumentation shall be designed to meet the following requirements:

- Automatically initiate the GDCS to prevent fuel-cladding temperatures from reaching the limits of 10 CFR 50.46.
- Respond to a need for emergency core cooling, following reactor depressurization, regardless of the physical location of the malfunction or break that causes the need.
- Be completely automatic in operation (i.e., no operator action required). Manual initiation of GDCS shall be possible at any time providing protective interlocks have been satisfied (i.e., the reactor is depressurized).

Nonsafety-related Design Bases

- No single control logic and instrumentation failure shall inadvertently open a GDCS valve, equalizing valve or deluge valve
- Instrumentation indicating GDCS valve positions and GDCS pool levels shall be displayed on a mimic of the system in the main control room.
- Alarm GDCS parameters in the main control room.

7.3.1.2.2 System Description

The basic components of the GDCS are within the containment. The GDCS pools, piping and valves are in the drywell. The suppression pool is on the outer periphery of the drywell within the containment envelope. The logic elements that provide controls for the actuation of the GDCS squib valves are outside the containment, in the four corners of the safety envelope that surrounds the drywell. The batteries and uninterruptible power supplies that provide ac and dc power to operate the system logic and actuate the squib valves are located in separate rooms inside the reactor building.

The GDCS pools are located within the drywell at an elevation significantly above the top of the active core. The suppression pool is located within the drywell with a water level a few meters above the top of active fuel (TAF).

Redundant safety-related level transmitters, two for each pool, continuously monitor the GDCS pool water level. These signals are continuously available on the safety related and nonsafety related displays and both high and low pool levels are alarmed by the plant computer functions (part of NE-DCIS).

Reactor Pressure Vessel (RPV) Level transducers used to initiate GDCS are part of the Nuclear Boiler System and are located on racks outside the drywell. The thermocouples that initiate the GDCS deluge valves are located in the lower drywell protective layer.

Actuation of GDCS injection sub-system is performed automatically, without need for operator action. It is also possible for the plant operator to manually initiate GDCS injection sub-system or to individually fire the various squib initiators independently by injecting trip signals to the automatic logic; the manual initiation is interlocked with reactor pressure to ensure that the GDCS pools can actually flood the reactor.

As previously described in the ADS logic section, the ECCS logic sends an initial start signal to the GDCS logic that will automatically initiate GDCS following reactor depressurization under LOCA conditions. After seal in, this signal represents either, reactor Level 1 OR reactor Level 1.5, and either simultaneous high drywell pressure OR a nominal fifteen minute timer time out, as shown in ECCS initiation signals of table 6.3-1.

Each of the two channels per division is presented with the initial start signal from the same ECCS logic that initiates ADS. The GDCS logic adds a time delay (Table 7.3-4, nominally 150 seconds) to the initial start signal and then operates all of the GDCS injection valves. Once the initial start signal is given to both ADS and GDCS (starting the various timers), the sequence is sealed in and cannot be aborted by the plant operator.

There are four GDCS injection lines coming from the three GDCS pools to the reactor vessel, one line per division. The squib valves on these lines are called GDCS injection valves and there are two valves on each line and two squib initiators per valve totaling eight GDCS injection valves and sixteen squib initiators. The logic divisions are evenly assigned to the squib initiators (each division has four squib initiators) such that a complete divisional failure will still result in all GDCS injection valves being fired.

There are four equalizing lines coming from the suppression pool to the reactor vessel, one line per division. The squib valves on these lines are called equalizing valves and there is one valve on each line and two squib initiators per valve totaling four equalizing valves and eight squib initiators. These equalizing valves are used after the GDCS flooded vessel's decay heat has boiled away sufficient inventory to again begin lowering level. After the initial start signal has been given (opening the ADS and GDCS valves) AND after an approximate half hour time delay (Table 7.3-4), AND when RPV water level drops below RPV Level 0.5 (1 m above TAF), the four equalizing squib valves mounted on the suppression pool equalizing lines are actuated. The logic divisions are evenly assigned to the squib initiators (each division has two squib initiators) such that a complete divisional failure will still result in all equalizing valves being fired. It is also possible for the operator to manually initiate the equalizing valves or to individually fire the various squib initiators independently by injecting trip signals to the automatic logic.

The GDCS pools also supply the deluge lines, which flood the containment floor after a severe accident. Actuation of the deluge valves is performed automatically with a backup capability for the operator to manually initiate the deluge valves. Automatic actuation of the deluge valves is thermocouple sensed lower drywell high temperature (see Table 7.3-4). There are 12 deluge valves with two squib initiators each; the logic divisions are evenly assigned to the squib initiators (each division has six squib initiators) such that a complete divisional failure will still result in all deluge valves being fired. It is also possible for the plant operator to manually initiate the deluge valves or to individually fire the various squib initiators independently by injecting trip signals to the automatic logic; the manual initiation is interlocked with drywell pressure to ensure that a severe accident condition exists.

The piping and instrumentation diagram is shown in Figure 6.3-2.

All of the above GDCS injection, equalizing and deluge valve logics include the same ECCS "division of sensors" bypass switch, 2 out of 4 trip decisions and single failure proof actuation logic. The valve logic is also single failure proof against inadvertent actuation such that each division of logic has two channels – each of which must operate for that division's valves to fire.

The same drywell pressure sensors and wide range level sensors are used as for the ADS logic and four divisional fuel zone range reactor level sensors are used for the equalizing valve logic; these are diverse from the sensors used for RPS functions and from those used by the diverse protection system. Both sets of transmitters belong to the Nuclear Boiler System.

The GDCS deluge lines are initiated by divisional thermocouple signals that generate an output trip signal within four deluge valve logic divisions.

The multiple deluge valve thermocouple signals are acquired per division by reactor building remote multiplexing units (RMUs) of the same division. The logic will require a certain number of thermocouples to be operational per division and will require a certain number to be above the

trip temperature before the divisional logic will generate a trip signal; in both cases the exact number will be determined in the detailed design phase.

The generation of the initial start signal for GDCS has been described in the ADS logic section. The logic for all squib initiators is similar. The signals are acquired per division by reactor building remote multiplexing units (RMUs) of the same division. The data are sent via fiber optics to the Safety System Logic and Control (SSLC) and logic cabinets located in the corresponding divisional I&C equipment rooms in the control building. Each division's logic compares the measured parameters to setpoints and outputs a "sensor" trip signal that is sent to its own division and each of the other divisions by appropriately isolated fiber optics.

Each division will therefore have access to the four divisional sensor trip signals and performs a 2/4 vote on the four sensor trip signals. The result of the 2-out-of-4 voting is sent redundantly to two separate trip logics channels in its own division and in each of the other divisions.

Each division will therefore have two separate trip logics that can independently perform a 2/4 vote on the sensor trips. The end result is that any two divisions sensing the appropriate trip conditions will result in all divisions providing a trip signal.

The existence of the two logic trips per division is necessitated by the requirement that no injection or equalizing squib valve be inadvertently fired by a single failure.

For the eight GDCS injection squib valves logic, each of the two (per division) initial start signals starts an adjustable timer with a preset nominal delay as specified in Table 7.3-4. After the time delay, each of the two timers will output a trip signal to the GDCS squib load drivers. Each of the four divisions has eight injection squib load drivers located in their corresponding reactor building RMU; there are eight injection squib valves and two squib initiators per valve.

Within the RMU, per squib initiator, there is a series circuit of 250 VDC divisional power, two load drivers in series, a current monitor and a normally closed keylock switch. Each of the two timers must transmit a trip signal to the corresponding series load driver. The effect is that both 2/4 trip voters, both timers and both load drivers must operate to fire the squib initiator, making the design single failure proof to inadvertently actuate. Because each GDCS injection squib valve always has two squib initiators, powered by different divisions, the design is also single failure proof to operate all eight valves.

The current monitor continuously verifies squib continuity, and the keylock switch is used when performing maintenance or surveillance testing or testing the current monitor. If the keylock switch opens the circuit, an alarm signal is sent to the control room to indicate the squib initiator (not the valve) is inoperable.

For diversity, the Diverse Protection System (DPS) also has the ability to fire one of the squib initiators on each of the eight GDCS injection squib valves using single failure proof (both to operate and to avoid inadvertent operation) logic. This is accomplished by paralleling the above described load drivers with two series switches that are operated by fiber isolated signals from the DPS system. (See Figure 7.3-1B.) The DPS system uses completely diverse sensors, hardware and software to operate the GDCS injection valves.

Any safety (for SSLC logic) or nonsafety (for DPS logic) Video Display Unit (VDU) in the Main Control Room (MCR) will be able to provide a display format that will allow the operator to

individually open a GDCS injection valve independently. These two manual opening schemes are completely diverse from one another.

Two control switches on the Division I MCR panels are furnished to allow the operator to manually open the four GDCS injection valves connected to Division I independently (using the primary GDCS logic). These switches will be of the “arm/fire” type and wired in series such that four deliberate operator actions (two for “arm” and two for “fire”) are required to operate the GDCS injection valves (this manual logic is interlocked with a low reactor pressure signal). A similar arrangement is provided for the one half of the GDCS injection valves operated by Division II. Similar to the ADS logic, any nonsafety VDU in the main control room will be able to provide a display format, which will allow the operator to individually open each GDCS injection valve independently by injecting trip signals to the DPS automatic logic. These display formats will require at least three deliberate operator actions per GDCS valve and is also interlocked with low reactor pressure. Finally four “arm/fire” switches (one per division) are furnished to manually initiate GDCS as a system instead of initiating each valve individually. If the operator uses any two of the four switches the GDCS sequence will seal in and start both the GDCS and equalizing valve sequencing; this will require four deliberate operator actions. For all of the manual initiations, operator use of the “arm” portion of the switch or display will cause a plant alarm.

For the four GDCS equalization squib valves logic, per division the initial start signal will each initiate a non-resettable longer equalization squib valve timer (Table 7.3-4). The outputs of the two equalization squib valve timers per division are combined with the two Level 0.5 signals per division such that any time Level 0.5 occurs after the end of equalization squib valve time delay, the logic will output a trip signal to the equalizing valve squib load drivers. Each of the four divisions has four equalizing valve squib load drivers located in their corresponding reactor building RMU; there are four equalizing valves and two squib initiators per valve. Figure 7.3-2 shows the initiation logic of a typical equalizing squib valve.

Within the RMU, per squib initiator, there is a series circuit of 250 VDC divisional power, two load drivers in series, a current monitor and a normally closed keylock switch. Each of the two equalization valve timers/Level 0.5 outputs must transmit a trip signal to the corresponding series load driver. The effect is that both 2-out-of-4 trip Level 0.5 voters, both timers and both load drivers must operate to fire the squib initiator, making the design single failure proof to inadvertently actuate. Because each equalizing valve always has two squib initiators powered by different divisions, the design is also single failure proof to operate all four valves. Because the equalizing valves are needed only long term, they are not operated by the DPS system. As previously described, they are included in the manual initiating GDCS valve logic and may also be fired individually.

The overall design of the system assures that all eight injection valves and all four equalizing valves will be fired even with a complete failure of a single division but no single failure will fire any squib.

The deluge valve logic is similar in that the lower drywell temperature data are sent via fiber optics to the Safety System Logic and Control (SSLC) and GDCS logic cabinets located in the corresponding divisional I&C equipment rooms in the control building. Each division's logic compares the measured temperature signal to an adjustable but nominal lower drywell high temperature setpoint (Table 7.3-4) and outputs a "sensor" trip signal that is sent to its own and to

each of the other divisions by appropriately isolated fiber optics. The trip signal is not sent until an adjustable but nominal two thermocouples per division exceed the setpoint.

Each division will therefore have access to the four divisional sensor trip signals and performs a 2-out-of-4 vote on the four sensor trip signals. The result of the 2-out-of-4 vote is sent redundantly to two separate trip logics in each of the other divisions.

Each division will therefore have two separate trip logics that can independently perform a 2-out-of-4 vote on the sensor trips. The output of these two "logic" trips (per division) is used as the "confirmed" temperature trip signal in all GDCS logic. The end result is that any two thermocouples in any two divisions sensing high drywell floor temperature will result in all divisions providing a confirmed temperature trip signal.

The existence of the two logic trips per division is necessitated by the requirement that no deluge valve be inadvertently fired by a single failure.

Each of the two (per division) temperature trip signals starts an adjustable but nominal deluge Squib valve non-bypassable timer. At the end of the deluge squib valve set time delay, each of the two timers will output a trip signal to the deluge valve squib load drivers. There are twelve total deluge valves (three per division) distributed between the GDCS pool discharge lines and two squib initiators per valve; each of the four divisions has six deluge squib load drivers located in their corresponding reactor building RMU.

Within the RMU, per squib, there is a series circuit of 250 VDC divisional power, two load drivers in series, a current monitor and a normally closed keylock switch. Each of the two timers must transmit a temperature trip signal to the corresponding series load driver, the effect is that both 2-out-of-4 trip voters, both timers and both load drivers must operate to fire the squib initiator - making the design single failure proof to inadvertently actuate. Because each deluge valve always has two squibs powered by different divisions, the design is also single failure proof to operate all twelve valves.

As with the GDCS and equalizing valves, the current monitor continuously verifies squib continuity and the keylock switch is used when performing maintenance or surveillance testing or testing the current monitor. If the keylock switch opens the circuit, an alarm signal is sent to the control room to indicate the squib initiator (not the valve) is inoperable.

The overall design of the system assures that all twelve deluge valves will be fired even with a complete failure of a single division but no single failure will fire any squib.

Two control switches on the Division I MCR panels are furnished to allow the operator to manually open the two equalizing valves connected to Division I independently by injecting trip signals to the GDCS equalizing valve automatic logic. These valves will be of the “arm/fire” type and wired in series such that four deliberate operator actions are required to operate the GDCS valves (this manual logic is interlocked with a low reactor pressure signal). A similar arrangement is provided for the one half of the equalizing valves operated by Division II. Any safety VDU in the main control room will be able to provide a display format that will allow the operator to individually open each equalizing valve independently by injecting trip signals to the automatic logic. These display formats will require at least three deliberate operator actions per equalizing valve. A similar arrangement is provided for the deluge valves except that the manual

control is interlocked with a high drywell pressure signal to assure a severe accident condition exists.

The resulting logic is such that, if both switches within Division I are operated, then half (two) of the equalizing valves will be fired. Similarly if both switches within Division II are operated, then the other half (two) of the equalizing valves will be fired. The "collar" part of the switch will also operate an alarm to indicate that the operator has "armed" the manual switches.

Similarly, if a high drywell pressure condition exists and both switches within Division I are operated, then half (six) of the deluge valves will be fired. Similarly if a high drywell pressure condition exists and both switches within Division II are operated, then the other half (six) of the deluge valves will be fired. The "collar" part of the switch will also operate an alarm to indicate that the operator has "armed" the manual switches.

7.3.1.2.3 Safety Evaluation

Section 6.3 evaluates the individual and combined capabilities of ADS and GDCS. For the entire range of nuclear process system break sizes, the Emergency Core Cooling Systems (ADS and GDCS) ensure that the reactor core is always covered.

Instrumentation that initiates the ADS and GDCS must respond to the potential inadequacy of core cooling regardless of the location of the breach in the reactor coolant boundary. Such a breach inside or outside the containment is sensed by reactor low water level and high drywell pressure. Because those signals are the only parameters that are completely independent of breach location, they are used to initiate the GDCS.

No operator action is required to initiate the correct response of the GDCS. If the system fails to initiate, the control room operator can manually accomplish GDCS initiation through switches and displays (with soft touch screen control) in the control room. Sufficient alarms and indications in the control room allow the operator to assess the performance of the GDCS. Specific instrumentation is addressed in Subsection 7.3.1.2.5.

The redundancy of the control and monitoring equipment for the GDCS is consistent with the redundancy of the four divisions of the GDCS. Control and monitoring equipment are located in the main control room and are under supervision of the control room operator.

No single failure in the initiating trip channel can prevent the initiation of the GDCS when required or inadvertently initiate the GDCS.

The initiation scheme for the GDCS is designed such that no single failure in the initiation circuitry can prevent the GDCS from providing the core with adequate cooling. This is caused by the redundancy of the components in the four divisions of the GDCS.

The GDCS has no equipment protective interlocks that could interrupt automatic system operation. To initiate the GDCS injection and equalization systems manually, a RPV low-pressure signal must be present. This prevents system initiation while the reactor is at operating pressure. To initiate the deluge lines manually, a high-high drywell pressure signal must be present. The high-high drywell pressure ensures that the deluge lines are actuated only during a severe accident. The GDCS is designed to operate from safety-related power. The system instrumentation is powered by divisionally separated, safety-related 120 VAC. The squib

valve/deluge valve logic and initiation circuitry is powered by divisionally separated, safety-related 250 VDC power.

The mechanical aspects of the GDCS are discussed in Subsection 6.3.2.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the instrumentation and control systems and the associated codes and standards applied in accordance with the Standard Review Plan. This table includes the GDCS and covers the codes and standards addressed in its design. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: GDCS complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. The GDCS is divisionalized and redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: GDCS demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

- 50.34(f)(2)(xiv)(II.E.4.2), Containment Isolation Systems

  Conformance: GDCS complies with this requirement.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail

  Conformance: The level of detail provided for the GDCS within the Tier 1 and Tier 2 documents conforms to this BTP.

- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.3 and Table 7.1-1, the following GDC are addressed for the GDCS:

Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24.

Conformance: The GDCS complies with these GDC.

Staff Requirements Memorandum (SRM

- SECY-93-087, Item II.Q, Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems

  Conformance: The GDCS conforms to these criteria in that diverse instrumentation and controls are provided, as described in Section 7.8

Regulatory Guides (RGs)

In accordance with the Standard Review Plan for Section 7.3 and Table 7.1-1, the following RGs are addressed for the GDCS:

RG 1.22 - Periodic Testing of Protection System Function - System logic is tested continually as described in Subsection 7.3.1.2.4. Components are tested periodically during refueling outages every two years. The GDCS fully complies with this RG.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems - The GDCS fully meets the requirements of RG 1.47. Automatic indication is provided in the control room to inform the operator that the system is inoperable or a division is bypassed.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems - The GDCS meets the requirements of RG 1.53 in addition to Section 5.1 of IEEE 603 and IEEE 379.

RG 1.62 - Manual Initiation of Protective Actions - The GDCS fully complies with this regulatory guide.

Each division of the GDCS has a manual actuation switch in the main control room. Initiation of two switches initiates the system. The switches ensure that the manual initiation of the system is a deliberate act. There is an interlock between the manual initiation switches and low reactor pressure that prevents manual initiation of the system if the reactor pressure vessel is not depressurized.

RG 1.75 - Physical Independence of Electric Systems - See Chapter 8 for general discussion of how the ESBWR meets RG 1.75.

Separation within the GDCS is such that controls, equipment, and wiring are segregated into four separate logic groups. Four dc power divisions provide redundant electrical power to the squib

valve firing circuits. One dc power division and two logic divisions are required for each squib valve to open. Refer to Subsection 7.3.1.2.2 for the design description of the GDCS initiation logic. Separation is provided to maintain the independence of the four divisions of the circuits and equipment so that the protection functions required during and following a design basis event can be accomplished.

The redundant equipment and circuits within the GDCS require divisional separation. Pertinent documents and drawings identify separation and safety-related status for each redundant division in a distinctive manner.

Redundant circuits and equipment are located within their respective divisional safety-related class enclosures. Separation is achieved by barriers, isolation devices or physical distance, which ensures that a single failure in one division would not affect the operation of the other redundant divisions.

The separation of redundant Class 1E circuits and equipment within GDCS is such that no physical connections are made between divisions except through nonmetallic fiber-optic medium.

Associated circuits are in accordance with Class 1E circuit requirements up to and including the isolation devices. Circuits beyond the isolation devices do not again become associated with Class 1E circuits.

Separation between Class 1E and non-Class 1E circuits either satisfies the same minimum requirements as for the separation between Class 1E circuits, or the circuits are treated as associated circuits.

RG 1.105 - Instrument Setpoints for Safety-Related Systems - The setpoints used to initiate GDCS are established consistent with this guide. A licensing topical report (Reference 7.2-1) provides the detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The GDCS complies with the intent of RG 1.118 as amplified in IEEE 338. A full functional test of the GDCS is not practical, because it would result in a loss-of-coolant event. Acceptable reliability of equipment operation is demonstrated by alternate test methods. System logic is self-tested every 30 minutes and a low-amperage current continuously tests the continuity of the bridge-wires within the squib valve actuating circuitry. Calibration verification of the GDCS and suppression pool level sensors can be conducted during plant operation because the level transmitters are located outside the drywell.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The GDCS fully complies with this regulatory guide.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control System (SSLC), Subsection 7.1.2.2.

Branch Technical Positions (BTP)

In accordance with the Standard Review Plan for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the GDCS:

BTP HICB-1 - Guidance on Isolation of the Low Pressure Systems from the High Pressure Reactor Coolant System - The GDCS design has the low pressure portion of the system

properly isolated from the high pressure portion of the system through two valves in series: a squib valve and a biased-open check valve that closes on very low differential pressure. This meets the intent of BTP for a necessary part of the Emergency Core Cooling System.

BTP HICB-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

This BTP is not applicable to the ESBWR, in that it has no reactor recirculation pump.

BTP HICB-6 – Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The ESBWR has no recirculation pump and has no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance on Application of Regulatory Guide 1.22 - This BTP requires the identification of actuated equipment not tested during reactor operation and a discussion of how each conforms to the provision of Paragraph D.4 of RG 1.22. In the GDCS, the squib valves are not actuated during reactor operation, because actuation of the squib valves would adversely affect the operation of the plant and would result in a reactor shutdown.

Given the GDCS system requirements for zero reactor pressure boundary leakage over the 60-year life of the plant, the only practical solution is for the system actuation valve to be a non-reclosing valve with a metal diaphragm seal that is ruptured to initiate system flow.

The GDCS is designed to provide adequate inventory make up to the core in the event of a LOCA. The system has sufficient redundancy and reliability that core-cooling requirements are met in the event of a LOCA.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices

SSLC logic controllers for GDCS use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

BTP HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

GDCS logic resides within the SSLC. The SSLC conforms to this BTP. Additional discussion is in Subsection 7.2.1.3.

BTP HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

This BTP does not apply to GDCS or SSLC. See Subsection 7.2.1.3 for additional discussion.

BTP HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 DFR Part 52

This BTP is applicable to all sections of the DCD including this section on GDCS. This section content conforms to this BTP.

BTPs 14, 17, 18, 19 and 21 are addressed in conjunction with the SSLC in Subsection 7.3.4.3.

TMI Action Plan Requirements

In accordance with the Standard Review Plan for Section 7.3 and Table 7.1-1, only TMI's I.D.3 and II.E.4.2 (addressed above) are considered applicable to the GDCS. Listed below are the TMI requirements that applied to previous ECCS systems in operating BWRs and license applicants that potentially could apply to the GDCS. Following each TMI is a brief discussion on why it does not apply to the GDCS:

TMI II.K.3(13) - HPCI and RCIC Initiation Levels - GDCS initiates on low-low water level and drains by gravity to the RPV. There is no high-level isolation or low-level restart with this system. This TMI item does not apply.

TMI II.K.3(15) - Isolation of HPCI and RCIC - This TMI applies to Emergency Core Cooling Systems with steam-driven pumps that use differential pressure sensors on elbow taps in the steam supply line to isolate the steam supply in the event of a pipe break. The GDCS uses gravity to produce system-driving head. The system has no steam-driven pumps. This TMI item does not apply to the GDCS.

TMI II.K.3(21) - Restart of Core Spray and Low Pressure Coolant Injection Systems - This TMI applies to Core Spray and Low Pressure Coolant Injection Systems that can be stopped by the operator. Once GDCS is initiated, the operator does not have the ability to stop it from completing the initiation sequence. This TMI item does not apply to GDCS.

TMI II.K.3(22) - Automatic Switchover of RCIC Suction - This TMI applies to reactor cooling systems that can take suction from multiple water sources. The GDCS takes suction from the GDCS pools and does not have the capability to manually or automatically switch over to an alternate source. This TMI item does not apply to the GDCS.

7.3.1.2.4 Testing and Inspection Requirements

The GDCS trip logic units are self-tested continually at preset intervals. The trip logic units of each logic division, and the timers for the automatic logic, may be tested during plant operation. GDCS equipment inside containment is tested during refueling outages. Refer to Subsection 6.3.2.7.4 for a discussion of mechanical tests performed on the GDCS.

7.3.1.2.5 Instrumentation Requirements

The performance and effectiveness of the GDCS in a postulated accident may be verified by observing the following control room indications:

- Status indication of locked-open maintenance valves;
- Status indication and alarm of the squib-actuated valves;
- Position indication of the GDCS check valves;
- Drywell and RPV pressure indication;
- Suppression pool high/low level alarm;
- GDCS pool high/low level alarm;
- Water level indication for the GDCS pools, suppression pools and RPV; and

- Squib valve open alarm.

The environmental capabilities of the GDCS instrumentation, located in the drywell that is essential for system operation, are designed to operate in a drywell environment resulting from a LOCA. The thermocouples that initiate the deluge valves are qualified to operate in the severe accident environment. Safety-related instruments, located outside the drywell, are qualified for the environment in which they must perform their safety-related function.

7.3.2 Passive Containment Cooling System

The Passive Containment Cooling System (PCCS) consists of heat exchanger loops that are an extension of the containment pressure boundary. The PCCS heat exchanger tubes are located in a pool of water (IC/PCC pool) outside the containment. A rise in containment (drywell) pressure above the pressure suppression pool (wetwell) pressure, as would occur during a loss of reactor coolant into the drywell, forces flow through the PCCS heat exchanger loops. Condensate from the PCCS drains to the GDCS pools. As the flow passes through the PCCS heat exchangers, heat is rejected to the IC/PCC pool, thus cooling the containment. This action occurs automatically without the need for actuation of components. The PCCS does not have instrumentation, control logic, or power-actuated valves, and does not need or use electrical power for its operation. Other information on the PCCS is given in Subsection 6.2.2.

7.3.3 Leak Detection and Isolation System

The primary function of the Leak Detection and Isolation System (LD&IS) is to detect and monitor leakage from the reactor coolant pressure boundary and to initiate the appropriate safety action to isolate the source of the leak from the containment. The system is designed to automatically initiate the isolation of certain designated process lines that traverse the containment to prevent release of radiological leakage from the reactor coolant pressure boundary. The initiation of the isolation functions results in the closure of the appropriate containment isolation valves.

7.3.3.1 System Design Bases

The following system design criteria are applicable to the design of LD&IS:

- The LD&IS is engineered as a safety system, Seismic Category 1, and shall conform to regulatory codes and standards listed in Table 7.1-1 for this system.
- Fail-safe design concepts shall be utilized in the logic design to allow containment isolation on loss of power to the plant.
- Isolation shall be initiated with precision and reliability once leakage has been detected from the reactor coolant pressure boundary.
- The loss of one divisional power source or one monitoring channel shall not cause inadvertent isolation of any containment valves.
- Once isolation is initiated, the isolation action shall go to completion. Deliberate operator action is required to return the system to normal and to reopen the isolation valves.

- The LD&IS design shall meet the single failure criteria; that is, no single failure within the system shall initiate inadvertent isolation or prevent isolation when required.
- Automatic isolation shall be initiated on a coincidence vote of any two-out-of-four channel trips as appropriate for each monitored variable.
- Sufficient electrical and mechanical separation shall be maintained between the divisional redundant instrumentation channels.
- The LD&IS design shall incorporate provisions to permit bypass of a single division of sensors at any one time.
- LD&IS instrumentation shall utilize a diversity of sensed parameters and redundant channels for initiation of containment isolation.
- Manual isolation capability shall be provided for diversity to the automatic logic.
- The containment leak detection methods that are described in RG 1.45 shall be considered and adopted in the LD&IS system design.
- Identified and unidentified leakages within the containment shall be monitored separately for quantifying the flow rates.
- The LD&IS shall provide different divisional isolation signals to the containment isolation valves.
- The control and isolation logic for the main steamline isolation valves (MSIVs) shall be provided in the LD&IS system design. The MSIV control logic for each pilot solenoid valve shall be as configured in Figure 7.2-1.

7.3.3.2 System Description

The LD&IS is a four-divisional system designed to detect and monitor leakage from the reactor coolant pressure boundary, and, in certain cases, isolate the source of the leak by initiating closure of the appropriate containment isolation valves. The LD&IS control and isolation logic utilizes two-out-of-four coincidence voting channels for each monitored plant variable for containment isolation. Various plant variables are monitored, such as flow, temperature, pressure, RPV water level, and radiation, and these are used in the logic to initiate alarms and the required control signals for containment isolation. Two or more diverse leakage parameters are monitored for each specific isolation function. The LD&IS logic functions reside in the framework of the Safety System and Logic Control System (SSLC), which generates the trip signals to initiate the isolation functions of the LD&IS.

The following control and isolation functions are implemented by the LD&IS:

- Containment isolation following a LOCA event;
- Main steamlines and drain lines;
- Isolation Condenser System process lines;
- RWCU/SDC System process lines;
- Fuel and Auxiliary Pools Cooling System process lines to the suppression and GDCS pools, and to the drywell sprays;

- Reactor Component Cooling Water System lines to drywell coolers;
- Drywell sumps liquid discharge lines;
- Containment purge and vent lines;
- Reactor Building area air supply and exhaust ducts; and
- Refueling area air supply and exhaust ducts.

The following leak detection and monitoring functions are implemented in the plant design:

- Condensate flow from the upper and lower drywell air coolers;
- Leakages in the drywell from valves equipped with leak off lines between the two valve stem packings;
- Fission products leakages into the drywell (by PRMS);
- Reactor Pressure Vessel head flange seal pressure leakage;
- Drywell sump levels and flow rates for identified and unidentified leakages; and
- SRV discharges into the suppression pool (by NBS).

The LD&IS control functions that initiate automatic isolation functions are classified safety-related, and these functions utilize redundant divisional channels that satisfy both the mechanical and electrical separation criteria and the single failure criteria. This system operates continuously during normal reactor operation, and during abnormal and accident plant conditions.

The system design is configured as shown in Figure 7.3-3. The LD&IS interfacing sensor parameters are provided in Table 7.3-5. Detailed description of detection methods, monitored plant parameters, and the monitoring instrumentation are covered in Subsection 5.2.5.

7.3.3.3 Safety Evaluation

The LD&IS control and isolation-functions, including the sensors and channel instrumentation, are engineered into a safety system and qualified environmentally and seismically for continuous operation during normal, abnormal, and accident plant conditions. The system design is in conformance with the design bases that are described in Subsection 7.3.3.1 and with the relevant codes and standards that are specified for this system in Table 7.1-1. LD&IS system design utilizes various measurements and redundant instrument channels to detect and monitor reactor coolant leakage in and external to the containment, and detect and isolate the source of the leak to prevent radioactive releases to the environs. The isolation logic utilizes four redundant divisional channels to monitor a leakage parameter, and uses the two-out-of-four coincidence voting logic technique for initiation of the isolation function. This design technique improves system availability to perform its safety functions, satisfies the single failure criterion, and permits channel bypass for maintenance and repair during normal plant operation. Loss of one channel due to failure or power loss does not cause inadvertent isolation.

The four redundant divisional channels of the LD&IS are a fail-safe design. The isolation logic is energized under normal conditions and de-energized to initiate the isolation function on indication of abnormal leakage.

The leakage detection methods associated with LD&IS logic functions generally comply with RG 1.45 with the Process Radiation Monitoring System performing the radiation monitoring of fission products. The RG 1.45 prescribes general guidelines to assure that leakage detection and collection system provides practical identification of leaks from the RCPB. The LD&IS logic is designed to seal-in the isolation signal once the trip has been initiated. The isolation signal overrides any control action to cause the closure of isolation valves. Reset of the isolation logic is required before any isolation valve can be manually opened.

The system logic design incorporates provisions to permit bypass of a single division of sensors at one time for repair and maintenance without affecting system capability to perform its safety function. While in the BYPASS mode, no other division of sensors can be bypassed simultaneously.

Manual control switches and associated logic are provided in the design of the LD&IS to give the operator the capability to perform manual control functions for initiation of isolation, logic reset, channel bypass and test functions.

The drywell low conductivity waste (LCW) and high conductivity waste (HCW) sumps instrumentation is designed to satisfy the leakage rate requirements for identified and unidentified sources. The LD&IS includes isolation logic that uses the discharge radiation of the LCW & HCW for the isolation of the drain lines that transfer waste sumps to the liquid radwaste system.

7.3.3.3.1 General Functional Requirements Conformance

Leak Detection and Isolation System is an instrumentation and control system that utilizes temperature, pressure, radiation, and flow sensor signals to detect, monitor, indicate and alarm leakages from the Reactor Coolant Pressure Boundary. The sensors are part of each individual system that provides input to Leak Detection and Isolation System.

7.3.3.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the Leak Detection and Isolation System function and the associated codes and standards applied in accordance with the Standard Review Plan (SRP) Table 7-1. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Exceptions or clarifications are noted.

10 CFR 50 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: LD&IS system complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. The Leak Detection and Isolation System consists of four divisions, which are redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: LD&IS demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

50.34(f)(2)(xiv)(II.E.4.2), TMI Action Plan Item IIE.4.2 Containment Isolation Systems

Conformance: LD&IS complies with this requirement.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail
- Conformance: The level of detail provided for the LD&IS in the Tier 1 and Tier 2 documents conform to this BTP.

- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC):

In accordance with Table 7.1-1, the following GDC are addressed for the Leak Detection and Isolation System:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, and 24

  Conformance: The Leak Detection and Isolation System comply with the GDC identified. GDC conformance is generically discussed in Subsection 3.1.

Staff Requirements Memoranda:

- Item II.Q, (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs)

  Conformance: The ESBWR Leak Detection and Isolation System and Engineered Safety Features (ESF) designs conform to the item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of diverse instrumentation and control, described in Section 7.8.

Regulatory Guides (RGs):

In accordance with Table 7.1-1, the following RGs are addressed for the Leak Detection and Isolation System:

- RG 1.22 RG Periodic Testing of Protection System Actuation Function
- RG 1.47 Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System
- RG 1.53 Application of the Single-Failure Criterion to Nuclear Power Protection Systems
- RG 1.62 Manual Initiation of Protective Actions
- RG 1.75 Physical Independence of Electric Systems
- RG 1.105 Setpoints for Safety-Related Instrumentation
- RG 1.118 Periodic Testing of Electric Power and Protection Systems
- RG 1.153 Power Instrumentation & Control Portions of Safety Systems

The Leak Detection and Isolation System conforms to all of the above listed RGs, with the assumption that the same interpretations and clarifications identified in Subsection 7.2.1.3 also apply to Leak Detection and Isolation System.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control System (SSLC)) in Subsection 7.3.4.3 and 7.1.2.2.

Branch Technical Positions (BTPs):

In accordance with the Standard Review Plan for Section 7.3, and with Table 7.1-1, the following BTP is addressed for Leak Detection and Isolation System:

- HICB-8 – Guidance for Application of RG 1.22
- HICB-11 – Guidance on Application and Qualification of Isolation Devices
- HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 – Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-19 – Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

- HICB-21 – Guidance on Digital Computer Real-Time Performance

Conformance: The Leak detection and Isolation system complies with the above HICBs. Discussion of HICBs 14, 17, 18, 19, and 21 are addressed in conjunction with the Safety System Logic and Control System (SSLC) in section 7.3.4.3, and in Subsection 7.1.2.2.

TMI Action Plan Requirements:

In accordance with the SRP for 7.3 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) and 10 CFR 50.34(f)(2)(xiv) (II.E.4.2) apply to the Leak Detection and Isolation System. The LD&IS complies with the requirements as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.3.3.4 Testing and Inspection Requirements

Inservice & Surveillance Tests

Inservice testing of the leak detection and monitoring channels is performed periodically to verify operability during normal plant operation and to assure that each tested channel can perform its intended design function. The surveillance tests include as required instrument channel checks, functional tests, verification of proper sensor and channel calibration, and response time tests in accordance with the established test procedures.

The LD&IS instrument channels utilize conventional sensors for leak detection and monitoring, and require no special or unique testing methods.

The setpoint verifications, the trip logic tests, and the channel integrity tests for the safety-related functions of LD&IS are processed and tested by the SSLC system.

MSIV Closure Tests

The LD&IS design provides manual capability and incorporates logic provisions to test closure of each of the MSIVs during normal reactor operation. To verify MSIV closure capability, each MSIV is periodically tested for partial closure while in service without causing a plant outage.

Testing and Maintenance in the Bypass Mode

Testing, calibration, and maintenance are performed in accordance with established procedures on the equipment during the time when the channel is out of service or has been deliberately bypassed.

7.3.3.5 Instrumentation Requirements

The LD&IS is an instrumentation system designed to detect and monitor leakage from the reactor coolant pressure boundary, using a diversity of parameters and redundant instrument channels. The monitored leakage parameters are provided continuously to the SSLC system for processing and initiation of the required trips for the isolation functions.

The LD&IS instrumentation requirements for each specific monitoring and isolation function are described in detail in Subsection 5.2.5. The plant parameters that are monitored for leakage detection, isolation, and alarms are summarized in Tables 5.2-8 and 5.2-9.

7.3.4 Safety System Logic and Control

7.3.4.1 Design Bases

The Safety System Logic and Control (SSLC) system performs the control logic processing of the plant sensor data and manual control switch signals that activate the functions of the Reactor Protection System (RPS), Leak Detection and Isolation System (LD&IS), Anticipated Transient Without Scram (ATWS) Mitigation Function by Standby Liquid Control (SLC) system, Emergency Core Cooling System (Gravity-Driven Cooling System (GDCS) and Automatic Depressurization System (ADS)) and a portion of the Safe Shutdown Systems (Isolation Condenser System (ICS)), and other safety-related functions.

The SSLC provides the following functions:

- Monitor safety-related signals that provide automatic control of the plant safety protection systems;
- Perform processing of plant sensor and equipment interlock signals according to the required trip and interlock logic, including time delays, of each safety-related interfacing plant system or system important to safe plant operation;
- Meet the performance requirements of each safety-related interfacing plant systemor system important to safe plant operation, including transient response, delay time, and overall time to trip system actuators or initiate necessary system operation;
- Monitor safety-related manual control switches used for system or component test, protection system manual initiation, and individual control of equipment actuators;
- Furnish trip outputs signals to actuators that drive safety system equipment, for example, solenoids and squib explosive-actuated valves;
- Furnish trip or initiation outputs signals to the logic of interfacing functions: Rod Control and Information System (RC&IS), Control Rod Drive (CRD) system, Standby Liquid Control (SLC) system, etc.;
- Monitor conditions for anticipated transient without scram (ATWS) and generate control outputs to systems that provide ATWS prevention and mitigation functions;
- Provide diagnostic facilities for detecting imminent failure of system components and provide an operator interface that facilitates quick repair;
- Provide alarm and status outputs to operator displays, annunciators and the plant computer; and
- Satisfy regulatory requirements for implementation of:
  - Single failure criterion;
  - Defense-in-depth protection;
  - Testability;
  - Separation and independence; and
  - Bypass of certain functions and indication of bypass.

7.3.4.2 System Description

SSLC is the decision-making control logic segment of the ESBWR's automatic protection and engineered safety features (ESF) systems. SSLC processes automatic and manual demands for reactor trip (scram), nuclear system isolation, ATWS/SLC system Initiation, and engineered safety features actuation based upon sensed plant process parameters or operator request. The SSLC includes the control and instrument that implements the protective functions of the Reactor Protection System (RPS), the isolation functions of the Leak Detection & Isolation System (LD&IS), the automatic depressurization system (ADS) functions of the Nuclear Boiler System (NBS) for safety relief valves (SRV) control and depressurization valve (DPV) control, the ESF functions of the Gravity Driven Cooling System (GDCS), and the shutdown and ESF functions of the Isolation Condenser System (ICS) and Standby Liquid Control System (SLC system).

General SSLC Arrangement

SSLC resides in four independent and separated instrumentation divisions. SSLC integrates the control logic of the safety-related systems in each division into firmware or microprocessor-based, software-controlled, processing modules located in divisional cabinets in the safety equipment room of the control building. SSLC runs without interruption in all modes of plant operation to support the required safety functions.

The SSLC consists of the reactor trip and MSIV isolation function (RTIF) part of the function, the LD&IS function, and the engineered safety features (ESF) part of the function. The SSLC/RTIF part includes the functions of the reactor protection system (RPS) and MSIV closure logic of leak detection & isolation system (LD&IS). The ESF part includes the functions of SRV and DPV initiation, the GDCS initiation, the shutdown cooling logic function of the ICS, the ATWS mitigation function (boron injection) performed by the Standby Liquid Control (SLC) System, as well as other associated logics. There are separate multiplexing networks for RTIF and ESF functions within each division. Figure 7.3-4 shows the functional block diagram of the SSLC/ESF portion of the system. The SSLC/RTIF RPS function is discussed in Subsection 7.2.1, with the RPS functional block diagram shown in Figure 7.2-1.

Most SSLC/ESF input data are process variables multiplexed via the Essential DCIS system (E-DCIS) in four physically and electrically isolated redundant instrumentation divisions (Subsection 7.9.1). Each of the four independent and separated E-DCIS channels feeds separate and independent channel of SSLC/ESF equipment in the same division.

Signal Logic Processing

Signals that must meet time response constraints, and signals from system logic that is in close proximity to the SSLC cabinets are directly connected to the divisional cabinets in the safety equipment room in the control building. These signals are derived from sensors that are redundant in the four divisions for each sensed variable. All input data are processed within the remote multiplexing unit (RMU) function of the E-DCIS. The sensor data is then transmitted through the DCIS network to the SSLC/ESF digital trip module (DTM) function for setpoint comparison. A trip signal is generated from this function. Processed trip signal from its own division and trip signals from other three divisions transmitted through communication interface are processed in the voter logic unit function (VLU) for 2-out-of-4 voting. The final trip signal is then transmitted to the RMU function via the E-DCIS network to initiate mechanical actuation

devices. There are two independent and redundant VLU functional channels in each division of the SSLC/ESF equipment. The vote logic trip signals from both VLU functional channels are transmitted to the RMU, where a 2-out-of-2 confirmation is performed. The redundant channels within a division are necessary to prevent single failures within a division from causing a squib initiator to fire; as a result both VLU logics are required to operate to get an output. Self-tests within the SSLC determine if any one VLU function has failed, and the failure is alarmed in the MCR. In order to prevent single instrumentation and control failure causing inadvertent actuations, a failed VLU function cannot be bypassed for any of the ECCS logic for squib valves initiation. Trip signals are hardwired from the RMU to the equipment actuator. The same logic process is performed for all four divisions and the resulting logic provides single failure proof actuation and single failure proof inadvertent actuation. The 4-division, 2-out-of-4 coincident signal voting occurs simultaneously for the equivalent signals in the four divisions. This arrangement provides multiple, independent trip channels to accommodate random single failure. The four divisions are interconnected by fiber optic communication links via a communication interface module. The fiber optic links provide electrical isolation for data transmission.

In summary, at the division level, the four redundant divisions provide a fault-tolerant architecture that allows single division of sensor bypass for on-line maintenance, testing, and repair without losing reliable trip capability. In such bypass condition, the system automatically defaults to 2-out-of-3 coincident voting when a division of sensor inputs is bypassed. The fault-tolerant arrangement thus conforms to safety system requirements for single failure tolerance, independence, and separation, as required by IEEE Std. 603.

SSLC/ESF does not require operator intervention during normal operation and allows manual bypass under abnormal conditions or required maintenance conditions, such as failure of sensors. Safety-critical automatic operations are provided with manual switches in each division for equipment initiation. Key safety RPS and ESF trip logics are duplicated in the Diverse Protection System (DPS), which addresses the common mode failure concern and protection of digital computer systems performing safety function. This system is described in Section 7.8.

The SSLC also includes the ATWS mitigation logic for liquid boron injection as a diverse means of shutting down the reactor. This ATWS mitigation logic for boron injection is implemented in the SSLC using non-microprocessor based discrete logic to provide circuitry diverse from the microprocessor-based SSLC logic. Other functions such as trip seal-in and reset, logic channel bypass, and other manual control functions also use non-microprocessor based circuitry.

Testing and maintenance activities are supported through the use of manual control switches that can activate the trip logic signal of each safety system. In addition, on-line self-diagnostic tests that check the critical performance of the digital control instrument are performed continuously within SSLC/ESF. An illustration of SSLC and its relationship to the RPS and other interfacing systems is shown in Figure 7.3-5.

The RPS trip logic uses “de-energized-to-trip” and “fail-safe” logic. The SSLC/ESF trip logic uses “energized-to-trip” and “fail-as-is” logic. The trip signal is transmitted via isolators (if required) and load drivers to the actuators for protective action. The load drivers are solid-state power switches, which direct appropriate currents to various devices, such as scram pilot valve solenoids, air-operated valves, and explosive-actuated squib valves. The logic is designed that once initiated automatically or manually, the intended sequence of protective actions will continue until completion. This satisfies the requirement of IEEE Std. 603.

More detailed descriptions of the SSLC/ESF trip logics for ADS and GDCS initiation are included in Subsection 7.3.1.

Division-of-Sensors Bypass

Bypassing any single division of sensors is accomplished from each divisional SSLC cabinet by manual switch control. This bypass disables the DTM outputs of a division at the associated voting logic inputs (VLU inputs) in the four divisions. Interlocks are provided so that only one division of sensors at a time can be placed in bypass. When such a bypass is made, all four divisions of 2-out-of-4 logic become 2-out-of-3 logic while bypass is maintained. Bypass permits calibration and repair of sensors or the DTM function. Even though all sensors for all systems are bypassed in one division, the remaining three divisions furnish sufficient redundant sensor data for safe operation and the logic is such that all four divisions can still perform 2-out-of-4 (2-out-of-3) trip decisions even if sensors are bypassed. Bypass status is indicated to the operator until the bypass condition is removed. An interlock rejects attempts to bypass simultaneously more than one SSLC division.

Division-out-of-service Bypass

For the fail-safe design (e.g., RPS), a division-out-of-service bypass inhibits the trip output in a division from affecting the output load drivers by maintaining that division's load drivers in an energized state. Bypass status is indicated to the operator until the bypass condition is removed. Only one division can be bypassed at any one time. For the ESF logic in the SSLC, since there is the division of sensor bypass implemented, and there are two channels of 2-out-of-4 VLU logic, no additional division trip logic bypass is implemented in the ESF logic. Each of the two VLU trip outputs is directly applied to one of the two load drivers in series. Both VLU trips are required to prevent inadvertent trip initiation of the squib valves. It is undesirable to perform the VLU logic bypass activities with the RMU electrically connected to the valve. The keylock switch that bypasses (disables) the load driver actuation provides effective bypass function required at the actuator level. (See Figure 7.3-1A and Figure 7.3-1B.)

7.3.4.3 Safety Evaluation

The four separated divisions of logic processing equipment provide the necessary degree of redundancy and independence to maintain safe operation despite the loss of portions of the processing capacity.

The SSLC system is designed so that no single equipment failure causes inability to:

- Perform reactor trip;
- Establish containment isolation; or
- Initiate the engineered safety features.

SSLC is a framework that consists of a set of logic processing functions for several safety-related systems and is therefore treated as a safety-related system. The functions related to sensor signal processing and trip output are safety-related.

Separation:

Physically separate divisions are established by their relationship to the reactor vessel, which is divided into four quadrants. The sensors, logic, and output actuators of the various systems are allocated to these divisions.

Diversity:

The digital devices in SSLC are, in general, microprocessor-based, software-controlled instruments. However, some system functions are provided with discrete, solid-state, non-microprocessor, logic cards in order to be consistent with the diversity of sensor inputs or actuated devices.

Discrete non-microprocessor based logic is used to activate the ATWS mitigation liquid boron injection functions (Figure 7.8-3) in the SSLC, while microprocessor based logic in the SSLC activates the solenoid-controlled safety relief valves, squib-actuated depressurization valves and GDCS valves. MSIV automatic closure on RPV Level 2 is backed up through discrete logic by a Level 1 closure signal. The Level 1 sensors are diverse from the other set of level sensors. Similarly, the same diverse level sensor through additional discrete logic backs up the containment isolation signals for several normally open valves.

For ESBWR, a diverse instrumentation and control system is incorporated which has a totally independent set of selected reactor trip logic functions and ESF initiation logic functions that address the requirements of BTP HICB-19 position. This system is described in Section 7.8.

Environment:

The SSLC system is designed to operate in a mild environment in clean areas within the control building and reactor building safety envelope. Refer to Chapter 9.4.6 for specific environmental conditions.

Panel internal environment are maintained to ensure that reliability goals are achieved. Panel internal cooling is by natural convection. Fans may be used to improve long-term reliability, but no credit is taken for forced-air cooling in the qualification of safety-related functions. Thermal design adequacy is considered during detail equipment design by analysis of heat loads (per circuit module, per bay, per module).

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the SSLC and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50.55a (IEEE 279)

- Conformance: IEEE Std 603 supercedes IEEE Std 279. Addressing RG 1.153 and IEEE 603 as discussed in Subsections 7.1.2.3.3, 7.1.2.3.6, and 7.2.1.2.4 (including design criteria discussions on quality, system integrity, independence, etc.) satisfies 10 CFR 50.55a(h) and IEEE Std 603. Additional information on SSLC equipment qualification is included in Reference 7.1-5.

10 CFR 50.34 (f)(2)(v)(I.D.3) Bypass and Inoperable Status Indication

- Conformance: This is discussed in Subsection 7.2.1.3 for the RPS, which is part of the SSLC function. The SSLC/ESF also demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

10 CFR 50.34 (f)(2)(xiv)

- Conformance: The SSLC logic that controls containment isolation functions conform to this criteria.

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

- Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

52.47(a)(1)(vii) Interface Requirements

- Conformance: Interface material is provided in Tier 1.

52.47(a)(2) Level of Detail

- Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this requirement.

52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

- Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

52.79(c) ITAAC in Combined License Applications

- Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following GDC are addressed for the SSLC:

- Criteria: GDC 1, 2, 4, 13, 19, 20, 21, 22, 23, 24
- Conformance: The SSLC complies with these GDC.

Staff Requirements Memoranda:

Item II.Q of SECY-93-087 (Defense Against Common-Mode Failures in Digital Instrument and Control Systems)

- Conformance: The ESBWR Reactor Trip (Protection) System and Engineered Safety Features (ESF) designs conform to Item II.Q of SECY-93-087 (BTP HICB-19) in conjunction with the implementation of the Diverse Protection System, described in Section 7.8.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following RGs are addressed for the SSLC:

RG 1.22 - Periodic Testing of Protection System Actuation Functions – The SSLC fully supports compliance with the guidance of RG 1.22.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems – SSLC provides bypass capability and status indication that includes Essential DCIS.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems – The SSLC meets the requirements of RG 1.53 in addition to Section 5.1 of IEEE 603 and IEEE 379.

RG 1.62 - Manual Initiation of Protective Actions – The SSLC meets the requirements of RG 1.62. These signals for manual initiation of protective actions are hardwired to the SSLC equipment.

RG 1.75 - Physical Independence of Electric Systems – The SSLC fully complies with the guidance of RG 1.75 and the requirements of IEEE 384.

RG 1.105 - Instrument Setpoints for Safety-Related Systems – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems – The SSLC conforms to RG 1.118 as amplified in IEEE 338. Testing of the SSLC is done in conjunction with the Essential DCIS.

RG 1.152 - Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants – The SSLC meets the requirements of RG 1.152 and ANSI/IEEE - ANS 7-4.3.2. Additional discussion is in Subsection 7.2.1.3, for RPS system compliance.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems – The SSLC in conjunction with the Essential DCIS fully conforms to this regulatory guide.

RG 1.168 - Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

RG 1.169 - Configuration Management Plans For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

RG 1.170 - Software Test Documentation For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

RG 1.171 - Software Unit Testing For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

RG 1.172 - Software Requirements Specifications For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

RG 1.173 - Developing Software Life Cycle Processes For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants – The SSLC fully complies with this guide, as delineated in Subsection 7.1.2.2. Additional discussion is included in Appendix 7B.

Branch Technical Positions (BTPs)

In accordance with the SRP for Section 7.3 and Table 7.1-1, the following BTPs are addressed for the SSLC:

BTP HICB-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps out of Service

This BTP is not applicable to the ESBWR, in that it has no reactor recirculation pump.

BTP HICB-6 – Guidance on Design of Instrumentation and Controls Provided to Accomplish Changeover from Injection to Recirculation Mode

The ESBWR has no recirculation pump and has no active ECCS pumps. Therefore, this BTP is not applicable.

BTP HICB-8 - Guidance on Application of Regulatory Guide 1.22

The SSLC is fully operational during reactor operation and is tested in conjunction with the Essential DCIS. Therefore, the Essential SSLC fully meets this BTP.

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices

SSLC logic controllers use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

Certain diverse and hardwired portions of RPS and SSLC may use coil-to-contact isolation of relays or contactors. This is acceptable according to the BTP when the application is analyzed or tested per the guidelines of RG 1.75 and RG 1.153.

BTP HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

The SSLC conforms to this BTP. Additional discussion is in Subsection 7.2.1.3.

BTP HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

This BTP does not apply to SSLC. See Subsection 7.2.1.3 for additional discussion.

BTP-HICB-14 - Guidance on Software Reviews for Digital Computer-based Instrumentation and Control

Safety Systems Development of software for the safety system functions within SSLC conforms to the guidance of this BTP as discussed in Appendix 7B. Safety-related software to be embedded in the memory of the SSLC controllers is developed according to a structured plan outlined in Appendix 7B.

BTP HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

This BTP is applicable to all sections of the DCD including this section on SSLC. This section content conforms to this BTP.

BTP-HICB-17 - Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems

The RPS and SSLC controllers conform to this BTP. Discussions on self-test and surveillance tests of RPS and SSLC are provided in Subsections 7.2.1.4 and 7.3.4.4.

BTP-HICB-18 - Guidance on Use of Programmable Logic Controllers [PLCs] in Digital Computer-based Instrumentation and Control Systems

Portions of SSLC design that use commercial grade PLCs for safety-related functions conform to this BTP (and to BTPs 14, 17, and 21) in that the PLCs will be qualified to a level commensurate with safety system requirements.

BTP-HICB-19 - Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

SSLC is a 4-division, independent and separated equipment arrangement. Isolation of signal transmission between safety-related divisions and between safety-related and nonsafety-related equipment employs non-conductive fiber-optic cable. System functions are segmented among multiple controllers. Automatic functions are backed up by diverse automatic and manual functions. Control system functions are separate, independent, and diverse from the protection system. Additional diverse features are included as discussed in Section 7.8, which describes the a diverse instrumentation and control system, specifically addresses the requirements of this BTP.

BTP-HICB-21 - Guidance on Evaluation of Digital System Architecture and Real-Time Performance

The real-time performance of SSLC in meeting the requirements for safety system trip and initiation response conforms to this BTP. Each SSLC controller operates independently and asynchronously with respect to other controllers. Maximum time delay from input to output is deterministic, based on the control logic design. Timing signals are not exchanged between divisions of independent equipment, nor between controllers within a division.

7.3.4.4 Testing and Inspection Requirements

A periodic, automatic self-test feature is included to verify proper operation of each SSLC logic processor. The self-test is an on-line, continuously operating self-diagnostics function. On-line self-test operates independently within each of the four SSLC divisions.

The major purpose of automatic self-test is to improve system availability by checking and confirming transmission path continuity for safety-critical signals, to verify operation of each 2-out-of-4 coincidence trip logic function, and to detect, alarm, and record the location of hardware or software faults. Tests verify the basic integrity of each card and the microprocessors. Discrete logic cards contain diagnostic circuitry that monitors critical points within the logic configuration and determines whether a discrepancy exists between an expected output and the

existing present state. The self-test operations are part of normal data processing and do not affect system response to incoming trip or initiation signals. Automatic initiation signals from plant sensors override an automatic test sequence and perform the required safety function. Process or logic signals are not changed as a result of self-test.

The self testing includes continuous error checking of transmitted and received data on the serial data links of each SSLC controller; for example, error checking by parity check, checksum, or cyclic redundancy checking (CRC) techniques. Self-test failures are alarmed to the operator at the main control room console and logged by the plant computer function of the NE-DCIS.

The following surveillance tests are performed on SSLC equipment:

(1) Sensor Channel (Instrument Channel) Check. Performance of this check provides confidence that a gross failure of a device in a sensor channel has not occurred. This check is continuously performed by the plant computer function and alarmed for divisional inconsistencies in sensor data; a visual comparison on the MCR main control console is also supported.

(2) Divisional Functional Test. A divisional functional test or channel functional test provides confidence that the software-based control programs within the SSLC controllers perform as intended. The test is performed by replacing the process signal with a test signal, which is generated by the SSLC test controller instrument. This test checks the function of the digital trip function and check trip logic and interlock logic response. The function of the DTM is checked with this test. This divisional functional test may be performed on-line with the sensor channel being tested bypassed. Because digital instrumentation is not expected to drift, the checks are of a confirmatory nature. This test is either automatic or semi-automatic and supplements the continuous self-diagnostic checks within each SSLC controller; for example the setpoints are continuously monitored by the plant computer function and alarmed when change is detected.

(3) Comprehensive Functional Test. This comprehensive test is performed during an outage (with a time interval specified by the Technical Specification). This test verifies overall SSLC system function, computer component function, software and hardware interactions, response times, and error handling in four divisions. This end-to-end test injects test signals simultaneously in the four divisions at the RMU inputs and to check the 2-out-of-4 voting logic (VLU) and other controller logics not checked during divisional functional test or automatic self-diagnostic checks. This test provides assurance that the protective action equipment is within its specified performance characteristics.

(4) Sensor Channel Calibration. This test verifies that a channel responds to the measured parameter within the necessary range and accuracy. Calibration is performed to the channel to account for any instrument drift. This calibration is performed during outages (with a time interval specified by the Technical Specification).

All test features adhere to the single-failure criterion, as follows:

- No single failure in the test circuitry incapacitates an SSLC safety function.
- No single failure in the test circuitry causes an inadvertent scram, MSIV closure, other PCV isolation, or actuation of any ESF system.

7.3.4.5 Instrumentation and Control Requirements

The SSLC equipment uses microprocessor-based programmable logic and control instrument, with standardized modules interchangeable with similar modules. Discrete solid-state logic is also used when applicable.

Control programs for each microprocessor-controlled instrument are in the form of software residing in non-volatile memory. The storage medium is in general Programmable Read-Only Memory (PROM). Programs are under the control of a real-time operating system residing in non-volatile memory. The equipment is qualified with verification and validation program conforming to applicable codes and standards.

Logic and controls for SSLC are located on each divisional SSLC cabinet in the equipment room in the Control Building, with key controls and system operating status available on the operator interface section in the main control room. The SSLC/ESF controls are used infrequently. Such controls normally do not require operator action during plant operation or during accident or transient conditions, and mainly are used for test and maintenance purposes. However, conditions such as equipment failure, maintenance, or testing, may require the operator to manually bypass a division of sensors or, for RPS/MSIV, a division of trip logic. Under the bypass status, SSLC continues to run in automatic mode using the unaffected logic in the remaining divisions.

The following minimum required SSLC/ESF displays are provided in the Main Control Room (per division):

- Division-of-sensors in bypass
- SSLC controller inoperative (DTM, VLU, or SLU)
- NIM, CIM, or Bridge Transfer Module (BTM) inoperative

7.3.5 COL Information

None.

7.3.6 References

None.

Table 7.3-1

Automatic Depressurization System Parameters

Parameter	Value
Number of ADS divisions	4
Number of separate logics (channels) per division	2
Number of logics (channels) within a division used to actuate the separate solenoid-operated gas pilots on each SRV	2
Number of logics (channels) within a division used to actuate the two separate igniter circuits on each squib-actuated DPV	2
Minimum number of ADS logic divisions to actuate any SRV pilot and open the SRV	2
Minimum number of ADS logic divisions to actuate (energize) one of the two igniter circuits and open the DPV	2
ADS trip logic units self-test time interval	continuous

Table 7.3-2

Safety-Relief Valve Initiation Parameters

Parameter	Value
Number of SRV groups	2
Number of SRVs in the first group (Group 1-initial ADS start signal)	5
Number of SRVs in the second group (Group 2 – second ADS start signal)	5
Time delay to confirm ECCS-LOCA signal, sec	10
Time after ECCS-LOCA confirmed initiating signal before signaling Group 1 ADS SRVs to open, sec	0
Time after ECCS-LOCA confirmed initiating signal before signaling Group 2 ADS SRVs to open, sec	10

Table 7.3-3

Automatic Depressurization Valve Parameters

Parameter	Value
Number of DPVs groups	4
Number of DPVs in Group 1 (third ADS start signal)	3
Number of DPVs in Group 2 (fourth ADS start signal)	2
Number of DPVs in Group 3 (fifth ADS start signal)	2
Number of DPVs in Group 4 (sixth ADS start signal)	1
Initial ADS time delay, after ECCS-LOCA confirmed initiating signal, before Group 1 DPVs are signaled to open, sec	50
Additional ADS time delay, after Group 1 initiation, before Group 2 DPVs are signaled to open, sec	50
Additional ADS time delay, after Group 2 initiation, before Group 3 DPVs are signaled to open, sec	50
Additional ADS time delay, after Group 3 initiation, before Group 4 DPVs are signaled to open, sec	50

Table 7.3-4

Gravity Driven Cooling System Parameters

Parameter	Value
Deluge squib valves initiated by lower drywell high temperature	>538°C (1000°F)
Injection squib valve time logic delay from initial start signal	150 s
Equalization line squib valve initiation logic time delay	30 min
Manual equalization squib valve initiation logic time delay	30 min

Table 7.3-5

LD&IS Interfacing Sensor Parameters

Temperatures:

- MSL Tunnel Area Temperature
- Drywell Temperature
- RWCU/SDC Valve Room Temperature
- MSL Temperature in Turbine Building (or alternate method)
- Isolation Condenser Area Room Temperature
- RWCU/SDC System Temperature

Pressures:

- MSL Turbine Inlet Low Pressure
- Main Condenser Low Vacuum
- Reactor Vessel Head Flange Seal Pressure Leakage
- Drywell Pressure

Radiation Levels:

- RCCWS Intersystem Leakage
- Drywell Fission Product
- Reactor Building HVAC Exhaust
- Refueling Handling Area Air Exhaust
- Drywell Sump Low Conductivity Waste (LCW) Drain Line to Radwaste
- Drywell Sump High Conductivity Waste (HCW) Drain Line to Radwaste
- Isolation Condensers Pool Vent Discharge

Flows:

- MSL Flow
- RWCU/SDC High Differential Volume Flow (Temperature Compensated)
- Drywell Air Cooler Condensate Flow
- Isolation Condenser Steam Line Flow
- Isolation Condenser Condensate Return Line Flow

Levels:

- Various RPV Water Levels
- Drywell and Containment Sump Levels

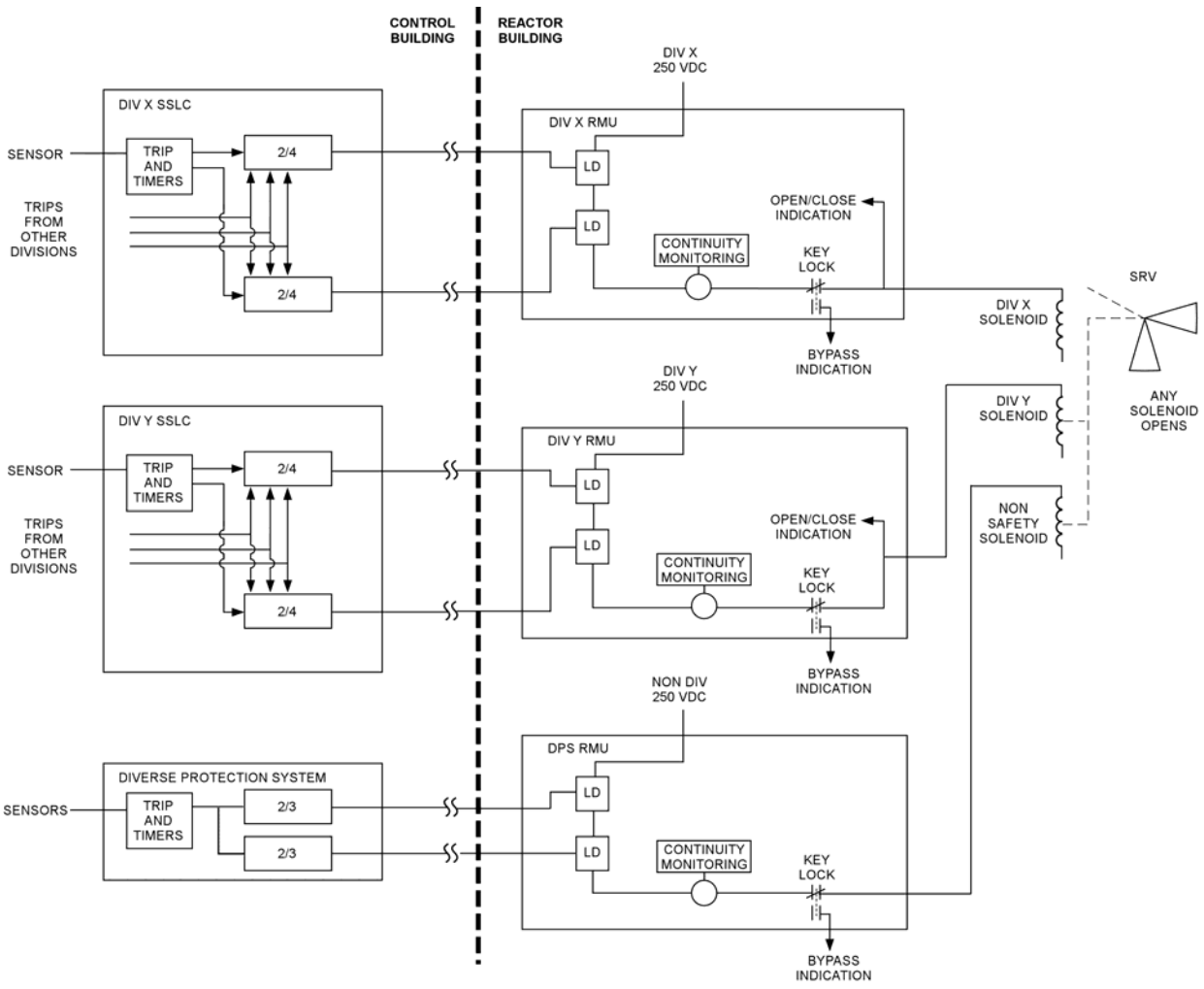


Figure 7.3-1A. SRV Initiation Logics

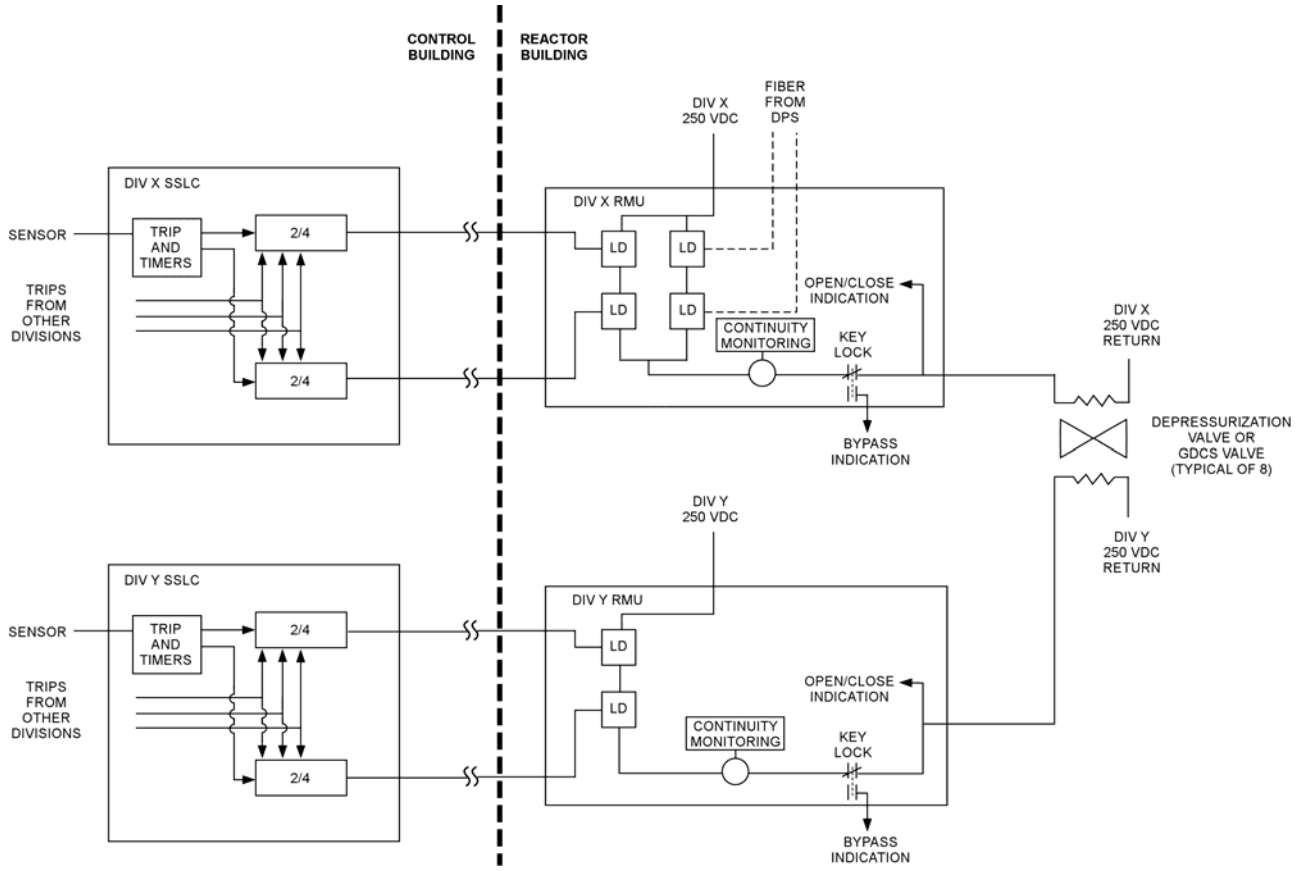


Figure 7.3-1B. GDCS and DPV Initiation Logics

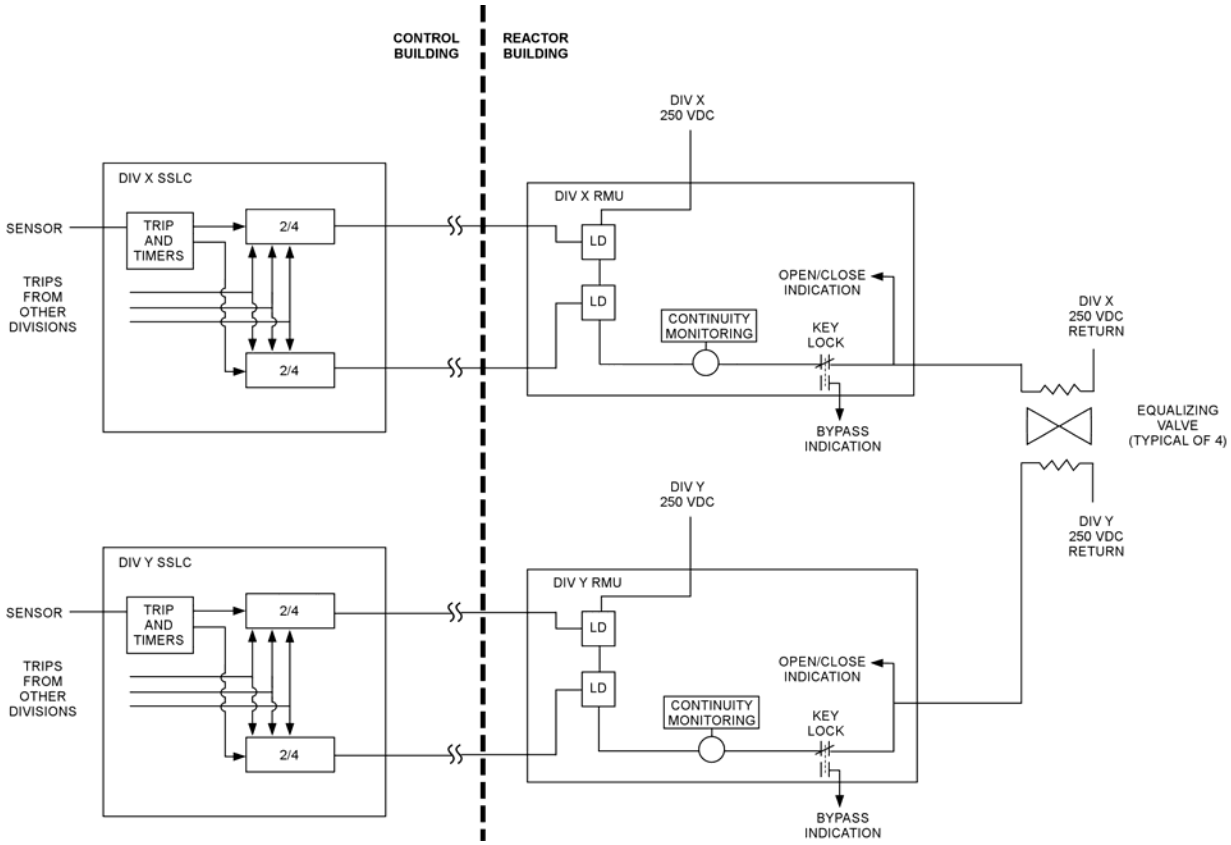


Figure 7.3-2. GDCS Equalizing Valve Initiation Logics

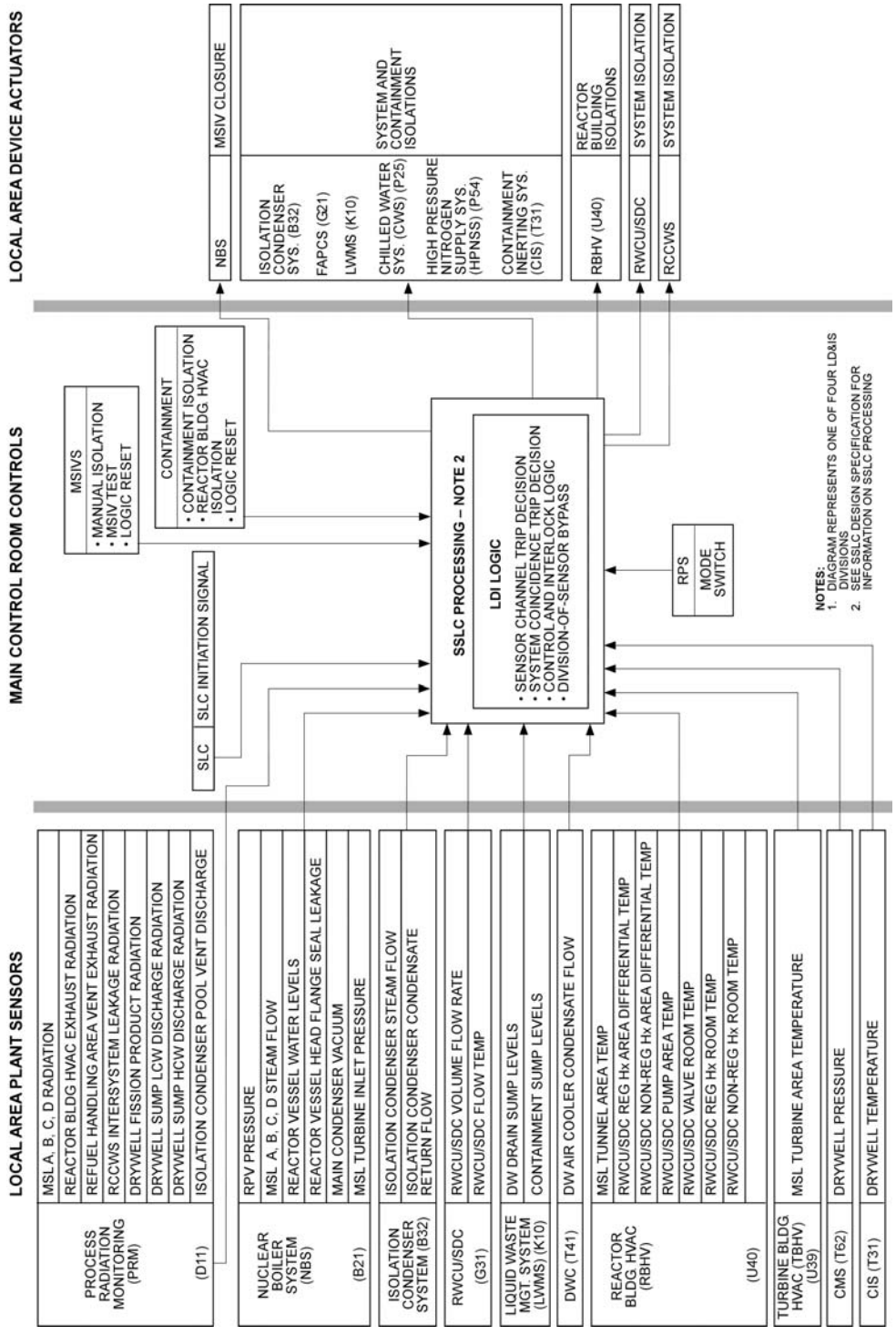
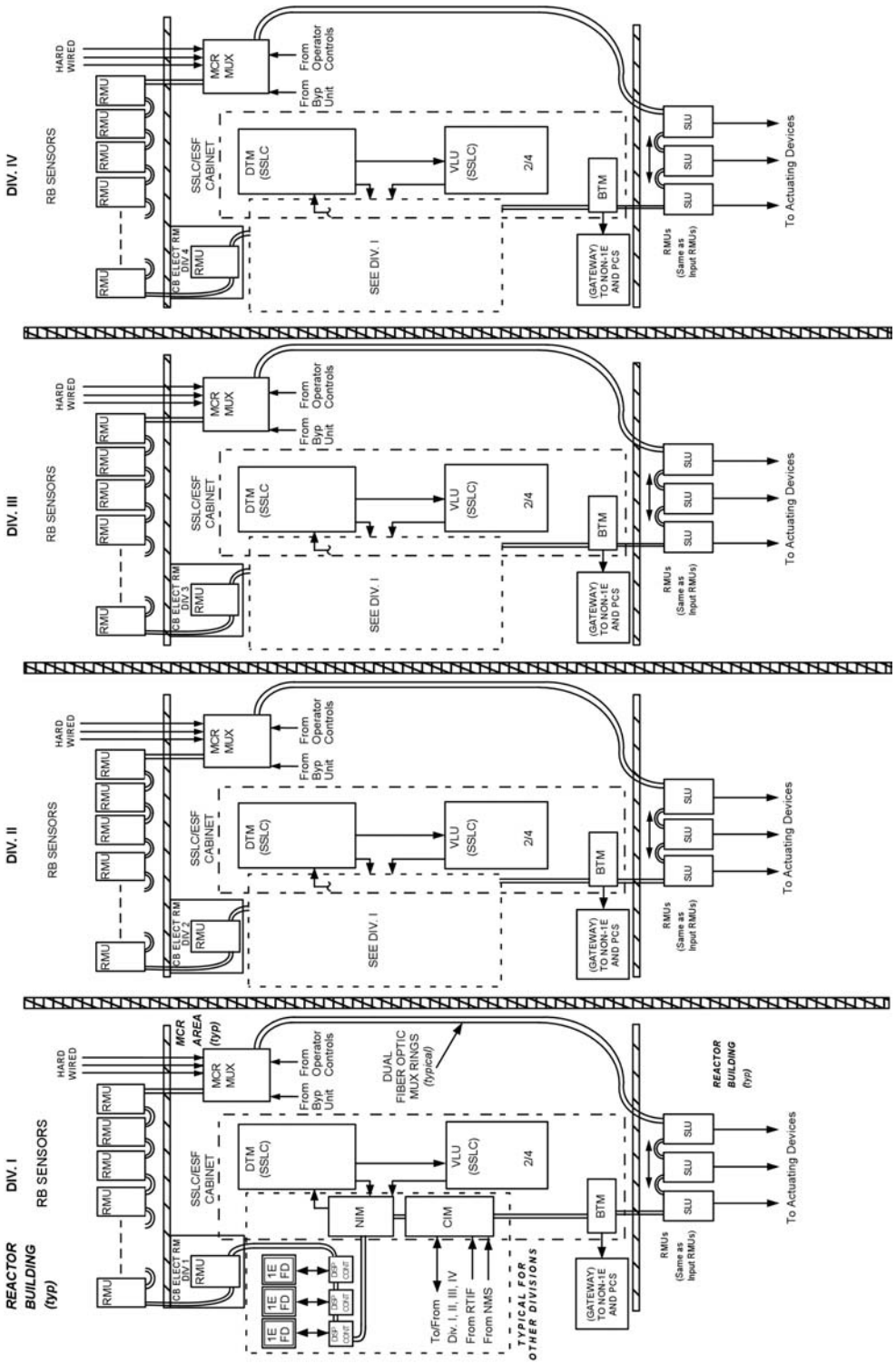
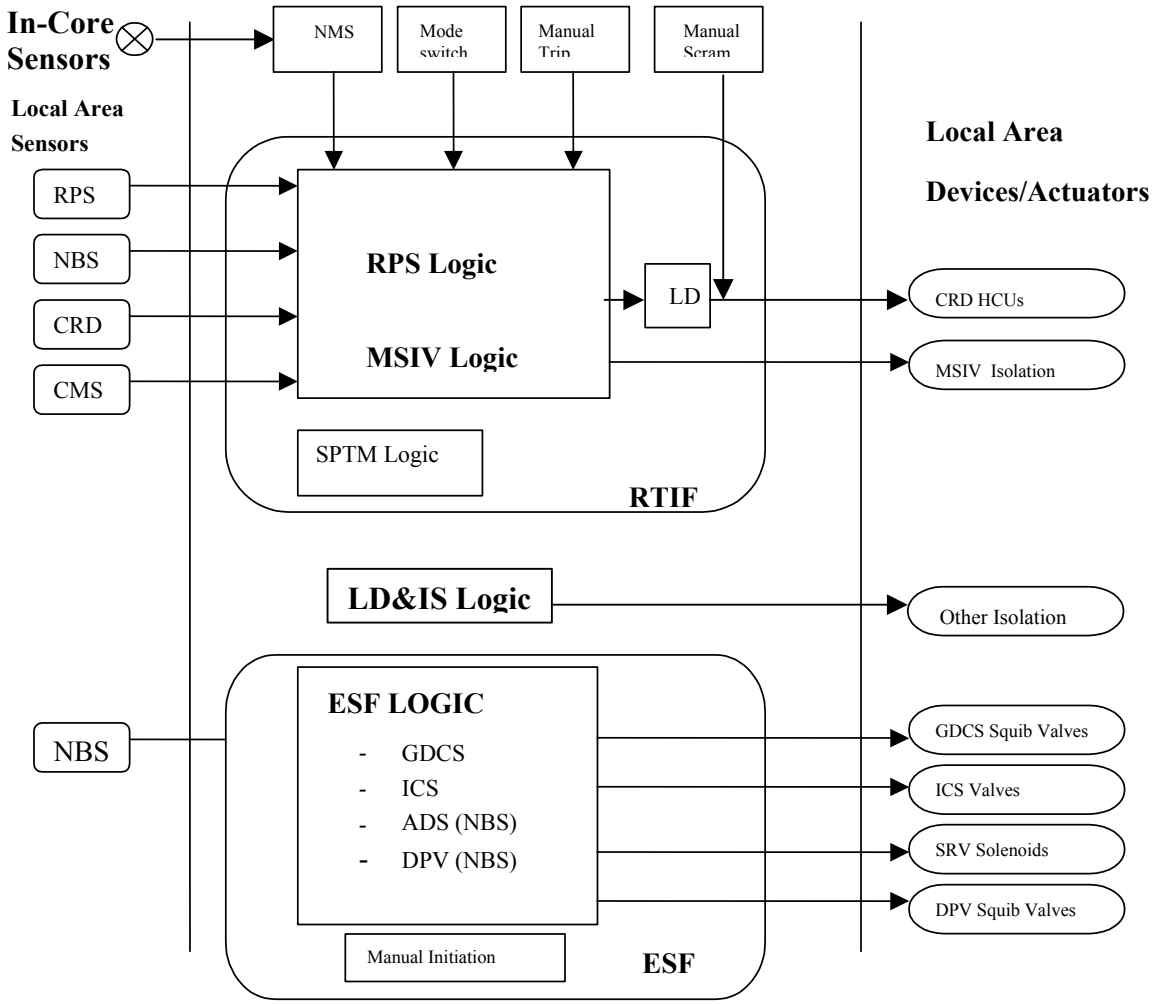


Figure 7.3-3. LD&IS System Design Configuration



(Note: the VLU contains dual redundant 2/4 logics with two independent trip outputs.)

Figure 7.3-4. SSLC Functional Block Diagram - ESF Portion



Note: 1) Local area sensors include:
RPS: turbine stop valve position, turbine CV oil pressure, turbine bypass valve position
NBS: MSIV position (for RTIF only), RPV pressure, water level
CRD: HCU accumulator charging water header pressure
CMS: drywell pressure
2) Manual Scram interrupts power to the circuit.
3) LD&IS resides in SSLC and shares sensors inputs with RTIP and ESF

Figure 7.3-5. SSLC System Interface Diagram

7.4 SAFETY-RELATED AND NONSAFETY-RELATED SHUTDOWN SYSTEMS

In accordance with the Standard Review Plan (SRP), this section includes "...those instrumentation and control systems associated with systems used to achieve and maintain a safe shutdown condition of the plant." However, some I&C systems that perform shutdown functions are not safety-related. This is justified by the existence of the safety-related systems (ICS, GDCS and PCCS), which utilize natural circulation in the performance of their cooling functions. Additionally, some safety criteria, such as redundant trains and single failure, have been utilized in the design of the nonsafety-related systems. Consequently, both safety-related and nonsafety-related systems that perform shutdown functions are addressed in this section.

7.4.1 Standby Liquid Control System

The Standby Liquid Control (SLC) system does not ensure any safety-related function, nor does it perform a safety-related function associated with any design basis event, as defined by 10 CFR 50.49(b)(1)(ii). However, for conservatism, the SLC system is classified as safety-related.

7.4.1.1 Design Bases

The SLC system design bases are presented within Subsection 9.3.5.

7.4.1.2 System Description

A detailed system description is given in Subsection 9.3.5.2. The control and instrumentation of the SLC system are described below. The SLC system is a manually initiated system, except during an Anticipated Transient Without Scram (ATWS) event or a LOCA event. The ATWS logic for SLC system system liquid boron injection initiation, which serves as a diverse emergency shutdown function (in compliance with requirements of 10 CFR 50.62), is addressed in Subsection 7.8 Diverse Instrumentation and Control Systems. The ATWS Mitigation SLC initiation logic is described in Figure 7.8-3. The LOCA initiation uses 2 out of 4 ECCS logic and automatically starts SLC system after receipt of an initial start signal (described in the ADS logic in Subsection 7.3.1.1) AND the first DPV (third ADS timer) injection signal. In all cases the SLC system logic and initiations are non-microprocessor based except for the SSLC originated start signal. The ATWS/SLC system logic is diverse from both ECCS and DPS sensors, hardware and software platforms; it is also diverse from the RPS hardware/software platforms.

Power Sources

Power for the safety functions of the SLC system is derived from the Class 1E 120 VAC and 250 VDC electrical systems. Divisional assignments are made to ensure independence of redundant components. The assignments used are listed below:

- Squib valves, F003 (A, C) and F003 (B, D) - Divisions I, II, III and IV,
- Shut-off valves, F002 (A, B) - Divisions I and II;
- Level instrumentation, N001, N002, R001 (A, C, E, G), (B, D, F, H) - Divisions I, II, III and IV; and
- Pressure instrumentation, N003, N004, N005, R002 (A, B) - Divisions I and II.

Control Functions

There are four control functions for the SLC system. Most important is the logic for firing of the two squib valves in each injection line. This is originated by the Safety System Logic and Control (SSLC) system. Successful firing of either or both squib valves in each SLC system loop assures adequate SLC system operation.

Control logic is also provided for manual venting of the accumulators. This function is not safety-related, except for preventing an unwanted venting. This is assured by provision of serial solenoid valves in each vent line, with each valve separately (jointly) actuated by respective remote manual switches. The initiation signals (switches) are manual from the control room.

Control logic is also provided for closure of the shut-off valves. This initiation is provided on a two-out-of-four logic basis using the level instrumentation for each accumulator when it indicates that the required neutron absorber solution inventory has been injected.

Automatic nitrogen makeup to the accumulators is provided to accommodate slow long-term leakage from the system. This makeup function is only required to maintain accumulator pressure, is not required to assure full solution injection, and, therefore, is not safety-related.

7.4.1.3 Safety Evaluation

The SLC system safety evaluation for the mechanical aspects of the SLC system is presented in Subsection 9.3.5.3. The SLC system also complies with the applicable general requirements for safety-related systems presented in Chapter 3. Electrical and I&C criteria applicable to the SLC system are identified in Table 7.1-1, and presented below.

10 CFR 50.55a(1) and 10 CFR 50.55a(h)

The SLC system complies with these criteria.

10 CFR 52.47

The SLC system, along with the other I&C systems in ESBWR comply with this criterion. See Subsection 7.1.2.2.

10 CFR 52.79(c) (ITAAC)

ITAAC are provided for I&C Equipment in Tier 1.

General Design Criteria

In accordance with the SRP for Subsection 7.4 and Table 7.1-1, the following GDC are addressed for the SLC system:

- Criteria: GDC 1, 2, 4, 13, 19 and 24
- Conformance: The SLC system complies with these GDC.

Regulatory Guides

In accordance with Table 7.1-1 and SRP Table 7-1, the following regulatory guides are addressed for the SLC system.

Regulatory Guide 1.53 - The SLC system is a redundant backup system to the reactor control and scram systems. For this reason, it is not required to withstand a single failure. Nevertheless,

this system has two redundant and parallel squib-type valves, only one of which is required for the safety-related function of SLC system. The SLC system instrumentation assuring operability of the system is also redundant.

Regulatory Guide 1.75 - The SLC system complies with RG 1.75.

Regulatory Guide 1.105 - The SLC system complies with RG 1.105 as delineated in Subsection 7.1.2.2.

Regulatory Guide 1.118 - The SLC system complies with RG 1.118.

Regulatory Guide 1.153 - Consistent with the discussion of other regulatory guides and the General Design Criteria, the SLC system complies with this regulatory guide.

Branch Technical Positions (BTPs)

HICB-11 - The approach to compliance with RG 1.75 and RG 1.153 is discussed above.

HICB-12 - The SLC system complies with BTP HICB-12.

HICB-16 - The level of detail provided for SLC system in Tier 1 and Tier 2 documentation complies with BTP HICB-16.

7.4.1.4 Testing and Inspection Requirements

An initial SLC system performance verification test is performed as a part of the startup test program. This test is intended to demonstrate that the SLC system performance is in accordance with the data provided in the process flow diagram.

A full test of this system is no longer possible after plant operation. There are, however, no active components in this system other than the two squib valves in each loop and only one valve in each loop is required. If one of the valves in each loop actuates with the system in its normal operating configuration and with critical system parameters (accumulator level and pressure) within their normal range, injection would occur as specified in the process flow diagram.

Normal surveillances assure operability with an acceptably low probability of demand failure.

7.4.1.5 Instrumentation Requirements

Status indications indicating full-open or full-closed valve positions are provided for the key valves in the SLC system. An open indication for these valves is required to assure SLC system operability.

Pressure and solution level alarms and indication for each accumulator are provided in the control room to:

- Ensure operability of the system;
- Warn of an out-of-tolerance condition on level or pressure; and
- Provide verification of proper system operation after initiation.

These measurements are redundant to minimize vulnerability to instrument or indicator failure. The level instrumentation for each accumulator is quadruple redundant in order to provide the two-out-of-four initiation signal for closure of the shut-off valve. The pressure indication and

alarm is dual redundant, and the signals from both channels are used for makeup of accumulator pressure. These instruments also provide local indication.

Local indication and control room alarm are provided for the nitrogen gas and poison solution makeup. The low level alarms are set to provide adequate time for recharging the manually operated nitrogen and sodium pentaborate solution supply systems.

7.4.2 Remote Shutdown System

7.4.2.1 Design Bases

The Remote Shutdown System (RSS) is a safety-related system used to provide operators with the means to safely shutdown the reactor from a place outside the Main Control Room (MCR) if the MCR becomes uninhabitable. RSS provides remote control of the systems that are needed to bring the reactor to a hot shutdown after a scram. RSS also provides the subsequent capability to bring the plant to and maintain the reactor plant in a cold shutdown condition. The specific regulatory requirements applicable to the RSS are listed in Table 7.1-1.

7.4.2.2 System Description

General

To achieve a safe and orderly plant shutdown from outside the main control room, controls and indicators necessary for operation of the following systems and equipment are provided on the remote shutdown panels. The controls and indicators necessary for operation of the following systems and equipment are provided on the remote shutdown panels. The RSS has two redundant and independent panels, each containing a safety-related digital visual display unit (VDU) whose power division corresponds to that of the RSS panel; provision is also made for performing a manual scram in the RSS. From these VDUs it is possible to control both safety-related and nonsafety-related systems as they would be controlled in the MCR for plant shutdown; all plant injection and cooldown systems are available depending only on the power available to run them. All plant signals can be monitored.

Signals required by RSS for display are sent from sensors to the RSS control panels where they are processed. Control signals from the MCR or the RSS control panels are transmitted to RMUs to operate the interfacing system's equipment The operational functions needed for remote shutdown control of a system are provided on the RSS control panels. All parameters that can be displayed and/or /controlled from Division 1 and Division 2 in the MCR, and that are necessary to follow the status of the reactor plant, are also displayed and/or /controlled from the corresponding divisional RSS panel.

All necessary power supply circuits are permanently active during plant operation. Therefore, RSS panel indications are always available for monitoring and control (although room access is under administrative control to prevent unauthorized entry and operation). The individual system equipment and instrumentation that interface with the RSS are listed on Table 7.4-1. A simplified RSS functional block diagram is provided in Figure 7.4-1.

The two RSS panels are located in two different areas and different rooms inside the Reactor Building (RB). The RSS panels are located in rooms that each have a sliding fire door with a minimum fire rating of 3 hours. The RSS panel room environment is normally similar to the

MCR environment. Access to and use of the RSS panels is administratively and procedurally controlled. This satisfies the control access requirement of IEEE Std. 603.

The RSS provides sufficient redundancy in the control and monitoring capability to accommodate a single failure in the interfacing systems and the RSS controls, in addition to the single-failure event that caused the control room evacuation. RSS is designed such that any failure within RSS does not degrade the capability of the interfacing systems. The RSS satisfies the single failure criterion and independence requirements of IEEE Std. 603.

Operating Conditions

The following conditions are assumed coincident with the event necessitating evacuation of the main control room and transfer of operation to the remote shutdown panel:

- The plant is operating under normal conditions. The initial plant power is less than or equal to rated power. No Anticipated Operational Occurrence (AOO), seismic event or other abnormal plant condition, except for loss of off-site power, is assumed.
- Backup power is available from nonsafety-related standby diesel generators and station batteries. The remote shutdown panel is powered from buses supplied by the standby diesel generators.
- The reactor operator can manually scram the reactor before leaving the main control room, and from the RSS either using the manual scram switches in the main control room RSS, or by opening the RRS logic input power breakers from outside the main control room.
- Plant personnel have evacuated the main control room.
- The RSS design includes control capability for reactor shutdown with or without isolation of the main steam lines.
- The reactor feedwater system, which is normally available, is conservatively assumed to be inoperable.
- The initiating event is assumed not to cause failure of the dc or ac control power supplies to the remote shutdown panel or failure of the dc or ac power feeds to equipment functionally controlled from the remote shutdown panel. This assumption is justified because the power feeds to the RSS do not pass through the main control room.

System Operation

When evacuation of the main control room is necessary, the reactor is manually scrammed, as described above under "Operating Conditions." The manual transfer displays on the remote shutdown panel VDUs are used to transfer control of the interfacing systems and equipment to the RSS. Normally, the turbine bypass valves automatically control reactor pressure, and the reactor feedwater system automatically maintains vessel water level. With these functions operable (and they should remain operable through the MCR evacuation), reactor cooldown is achieved through the normal heat sinks. This cooldown process can be supplemented from the remote shutdown panel using the RWCU/SDC system. The RWCU/SDC system provides the capability to bring the reactor from high-pressure conditions to cold shutdown. Control of both RWCU/SDC trains is provided on the remote shutdown panel. The Reactor Component Cooling

Water System (RCCWS) is aligned to provide cooling water to the RWCU/SDC non-regenerative heat exchangers, and the PSW system is aligned to cool the RCCW heat exchangers. Control of two RCCW trains and two PSW trains is provided on the remote shutdown panel.

If the reactor feedwater system is not available, control of the CRD system is provided on the remote shutdown panels. Control of the high-pressure makeup injection capability of the CRD system ensures that the vessel water level remains above the Automatic Depressurization System trip setpoint and above the elevation of the RWCU/SDC mid-vessel suction line nozzle. Control of both CRD trains is provided on the RSS panels.

If main steam line isolation occurs, the ICS automatically controls reactor pressure. Because the logic processing equipment for the ICS (or any other safety or nonsafety-related system) is not located in either the Reactor or Control Building but outside is located in either the Reactor or Control Building but outside the Main Control Room, ICS operation is not affected by an event necessitating control room evacuation, and continued operation of the isolation condensers is assumed. If the event necessitating control room evacuation results in a loss of the pressure regulator, but does not cause main steam line isolation, the ICS would initiate on high pressure. With the ICS in operation, the isolation condensers provide initial decay heat removal, and further reactor cooldown is achieved from the remote shutdown panels using the RWCU/SDC.

Additional information regarding operation of the systems that interface with the RSS is provided in the respective system descriptions.

7.4.2.3 Safety Evaluation

The RSS is classified as a safety-related system since RSS can control nuclear safety-related systems or equipment.

The RSS provides instrumentation and controls outside the main control room to allow prompt hot shutdown of the reactor after a scram and to maintain safe conditions during hot shutdown. It also provides capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the RSS and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR Parts 50 and 52

- 50.55a(h) Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Std 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 279 and RG 1.75.

  With regard to Paragraph 4.2 of IEEE 279, an event is assumed to have occurred to cause the evacuation of the control room. The RSS is designed to accommodate a single failure

in the interfacing systems or RSS controls for those scenarios. The effects of such failures are analyzed below.

The loss of one complete RWCU/SDC, RCCW or PSW loop could extend the time needed for the reactor to reach cold shutdown conditions. However, the ability of the RSS to ultimately facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal mode, and each RCCW and PSW train provides approximately 50% capacity for shutdown cooling mode. The RWCU/SDC, RCCW and PSW systems, in conjunction with the ICS, can bring the plant to cold shutdown within 36 hours, assuming the most restrictive single active failure.

In the event that one CRD train fails or is out of service for maintenance, the capacity of the remaining pump can provide sufficient makeup to maintain vessel water level during reactor cooldown.

Other sections of IEEE 279 that relate to testability of sensors, etc., are not applicable to the RSS.

- 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

  Conformance: RSS conforms in that there are no unresolved issues for RSS. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi) ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1. Test, inspection, analyses, and acceptance criteria of the RSS are identified in Tier 1.

- 52.47(a)(1)(vii) Interface Requirements

  Conformance: Design interface requirements during the licensing certification and design phases shall be commensurate with the detail required to support the completion of the final safety analysis and design-specific probabilistic risk assessment. Interface material is provided in Tier 1.

- 52.47(a)(2) Level of Detail

  Conformance: The level of detail provided for the RSS within the Tier 1 and Tier 2 documents conforms with this requirement

- 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c) ITAAC in Combined Operating License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1. No additional ITAAC for the I&C or RSS are required at the time of COL.

General Design Criteria (GDC)

In accordance with the SRP for 7.4, and with Table 7.1-1, the following GDCs are addressed for the RSS:

- Criteria: GDCs 1, 2, 4, 13, 19, and 24.

Conformance: The RSS complies with the GDC identified. GDC conformance is generically discussed in Section 3.1.

Regulatory Guides (RGs)

In accordance with the SRP for 7.4, and with Table 7.1-1, the following RGs are addressed for the RSS:

- RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 279 and RG 1.75. With regard to Paragraph 4.2 of IEEE 279, a single-failure event is assumed to have occurred to cause the evacuation of the control room. The RSS is designed to accommodate an additional failure in the interfacing systems or RSS controls for those scenarios. The effects of such failures are analyzed below.

  The loss of one complete RWCU/SDC, RCCW or PSW loop could extend the time needed for the reactor to reach cold shutdown conditions. However, the ability of the RSS to ultimately facilitate such conditions is not impaired. Each RWCU/SDC loop provides 50% capacity for residual heat removal mode, and each RCCW and PSW train provides approximately 50% capacity for shutdown cooling mode. The RWCU/SDC, RCCW and PSW systems, in conjunction with the ICS, can bring the plant to cold shutdown within 36 hours, assuming the most restrictive single active failure. In the event that one CRD train fails or is out of service for maintenance, the capacity of the remaining pump can provide sufficient makeup to maintain vessel water level during reactor cooldown.

  Other sections of IEEE 279 that relate to testability of sensors, etc., are not applicable to the RSS. The RSS complies with RG 1.53.

- RG 1.75 - Physical Independence of Electric Systems

  Conformance: The RSS complies with RG 1.75.

- RG 1.118 – Periodic Testing of Electric Power and Protection Systems

  Conformance: The RSS complies with RG 1.118.

- RG 1.152 - Digital Computers in Safety Systems

- RG 1.153 - Power Instrumentation & Control Portions of Safety Systems

  Conformance: The RSS complies with RG 1.153.

- RG 1.168 - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

- RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

- RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

- RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants
- RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control (SSLC) system in Subsection 7.3.4, the E-DCIS in Subsection 7.9.1, and in Subsection 7.1.2.2. The RSS is in compliance with these Reg. Guides.

Branch Technical Positions (BTPs)

In accordance with the SRP 7.4, and with Table 7.1-1, the following BTPs are applicable for the RSS:

- HICB-11 - Guidance on Application and Qualification of Isolation Devices
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 - Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 - Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 - Guidance on the Use of Programmable Logic Controllers in Digital

Computer-Based Instrumentation and Control Systems

- HICB-21 - Guidance on Digital Computer Real-Time Performance

  Conformance: The RSS complies with all the above HICBs. Discussion for HICB 14, 17, 18 and 21 are addressed in conjunction with the Safety System Logic and Control System (SSLC) in Subsection 7.3.4 and in Subsection 7.1.2.2.

TMI Action Plan Requirements

In accordance with the SRP for 7.4 and with Table 7.1-1, there are no TMI action plan requirements applicable for the RSS. However, TMI action plan requirements are generically addressed in Appendix 1A.

From the foregoing analysis, it is concluded that the RSS meets its design bases.

7.4.2.4 Testing and Inspection Requirements

The capability to safely shut down the reactor from outside the main control room shall be confirmed during the Initial Plant Test Program (Section 14.2). Testing to confirm the functionality of each RSS control circuit will be performed during each refueling outage.

7.4.2.5 Instrumentation Requirements

Process instrumentation in other plant systems provides the information for RSS operation. The instrumentation interface requirements are included in Table 7.4-1.

7.4.3 Reactor Water Cleanup/Shutdown Cooling System

7.4.3.1 Design Bases

Safety-Related Design Bases

The RWCU/SDC system functions are not safety-related. Therefore, the RWCU/SDC system has no safety-related design bases other than a containment isolation function and providing instrumentation for detection of system breaks outside the containment. The containment is isolated by signals from the LD&IS as described in Subsection 7.3.3 and the water purification equipment of the RWCU/SDC system is also isolated by signals from LD&IS received from the Standby Liquid Control (SLC) system.

Power Generation Design Bases

The RWCU/SDC system instrumentation shall be designed to provide suitable process indication, alarms, and manual and automatic devices for controlling the system as it:

- Removes impurities;
- Limits excess reactor water level during reactor heatup, startup, shutdown cooling and hot standby modes of plant operation;
- Minimizes reactor temperature gradients;
- Heats the reactor pressure vessel (RPV) for hydrostatic tests; and
- Removes reactor core decay heat during normal plant shutdowns.

The reactor water cleanup design bases are described further in Subsection 5.4.8.1.

This shutdown cooling design basis is described in further detail in Subsection 5.4.8.2.

7.4.3.2 System Description

Summary Description

The RWCU/SDC system performs essentially three basic plant functions. It provides a continuous purifying treatment of the reactor water during startup, normal operation, cooldown, hot standby, and shutdown modes of plant operation. It also removes core decay heat in conjunction with the main condenser or the isolation condensers during plant shutdown modes. Thirdly, the system (with the feedwater system) provides reactor vessel heat-up during cold start-up. There are two redundant RWCU/SDC trains. The overall functional description of the RWCU/SDC system is contained in Subsection 5.4.8. The instrumentation maintains the RWCU/SDC system process conditions within the limits necessary to control the system and satisfy the design bases. Protective features include isolating the RWCU/SDC system from the RPV with a LD&IS signal present The above isolation features protect the reactor core by minimizing the potential loss of RPV coolant inventory or by avoiding removal of boron from the RPV coolant if the SLC system is actuated.

Detailed System Description

General - The RWCU/SDC system instrumentation for flow, pressure, temperature, and conductivity are recorded or indicated with suitable alarms in the main control room. Valves

behind shielding are furnished with on-off air operators that are individually controlled from local panels or by extension stems that penetrate the shielding.

Indicating and control instruments and components are mounted on panels or local racks and are visible and accessible for repair, calibration, and testing.

Pumps - The main process pumps are manually started from the main control room by VDU control with status indication. The pumps are driven by solid-state type adjustable speed drives. Temperature elements located in the Nuclear Boiler System, and a reactor cooldown controller with temperature feedback processor control each pump to limit the rate of reactor water cooldown. A low pump suction flow interlock either prevents the pumps from starting or runs back or stops the pumps automatically. A reactor low water level (Level 3) pump speed runback interlock is provided to protect the pump from cavitation during shutdown.

The pumps are supplied from separate normal power sources. The pumps' power supplies are automatically switched to separate on-site standby diesel-generators on loss of preferred power (LOPP).

Power-Operated Valves - Motor-operated valves are manually operable from the main control room by a VDU switch. Each valve motor is stopped by limit switches or by torque switches. The positions of air/nitrogen-operated containment isolation valves are indicated in the main control room to permit the plant operators to assess their status. An Automatic signal overrides a manual signal to these valves. Containment isolation valve closing speeds are selected to protect the reactor core and limit radioactivity release in case of a RWCU/SDC system pipe break outside containment.

The following signals prevent all containment isolation valves with the exception of reactor bottom suction sampling line containment isolation valves from opening (if closed), or close them (when open):

- SLC system actuation sent to RWCU/SDC system via LD&IS; and
- LD&IS actuation.

The reactor bottom suction sampling line containment isolation valves isolation signal from LD&IS may be overridden by a manual opening signal when a reactor bottom fluid sample is required for post-accident sampling purpose.

The plant LD&IS, including the portion related to the RWCU/SDC system, is further described in Subsection 7.3.3.

Control Valves - A flow control valve is located on the RWCU/SDC system suction line from the upper RPV nozzle that controls flow from the upper RPV region. These flows are set manually using a flow controller located in the control room. Using thermocouples on the RPV bottom head drain line and the system suction line, the control valve from the RPV upper region is throttled during certain modes of plant operation (e.g., hot standby, startup, shutdown) to maintain the temperature difference across the vessel to within limits set by the plant Technical Specifications. The valve actuator is air-operated. The RWCU/SDC system also has a dump, or "overboarding," control valve to maintain RPV water level during certain modes of plant operation. This excess water is typically overboarded to the main condenser (Subsection 5.4.8). The valve is operated using instrument air and controlled both manually and automatically from

the control room using a controller and flow indicator. Pressure switches or transmitters located downstream of the overboarding valve protect low pressure components by alarming in the control room on high pressure and closing the throttle valve with a high-high pressure signal. When the overboarding valve is used during high-pressure RPV conditions (e.g., HOT STANDBY mode), a downstream orifice is used to assist in reducing system pressure; otherwise, the orifice is bypassed using a motor-operated valve. The overboarding throttle valve fails closed upon loss of power or air pressure.

The demineralizer bypass piping have an air-operated modulating flow control valve that will bypass the excess flow above the demineralizer capacity. The demineralizer is protected from over-temperature by automatic controls that first open the demineralizer bypass valve, and then close the demineralizer inlet valve.

Conductivity - Conductivity cells are located in the influent and effluent process sample streams of the demineralizers. These detectors are located in sample systems, which cool the sample stream to a constant temperature of 25°C (77°F); hence, conductivity elements are not required to be temperature compensated. Influent and effluent conductivity are continuously measured and transmitted to control room recorders. Measured values in excess of water quality requirements are alarmed in the control room.

Soluble and insoluble radioisotopic concentrations - The reactor water is manually sampled during cooldown, flood-up, or early period of fuel off-loading when activated corrosion product spiking may occur.

Temperature - Temperature elements are provided in the RPV bottom drain, the regenerative heat exchanger supply inlet and outlet, the non-regenerative heat exchanger outlet, the demineralizer influent (located at the pump suction), and the inlet and outlet of the regenerative heat exchanger return flow.

Temperature elements located in the Nuclear Boiler System, and a reactor cooldown controller with a temperature feedback processor, are utilized to provide the necessary signals to control the pump speed during cooldown to maintain the cooldown rate.

Flow - Density compensated system mass flow is measured in the process lines from the reactor bottom and mid-vessel nozzles with venturi-type flow element in each line and are located inside the containment. Flow elements are also provided in the seismic Category I RWCU/SDC return lines to the feedwater lines and the overboarding lines. The flow transmitters for all of these flow elements are arranged in two-out-of-four logic configuration, that are utilized to detect high RWCU/SDC differential mass flow due to a break outside the containment, and close the inboard and outboard containment isolation valves of the affected RWCU/SDC train. The containment isolation function on detection of RWCU/SDC high differential mass flow due to a break outside the containment is part of the LD&IS described in Subsection 7.3.3. See Figures 7.4-2A through Figure 7.4-2E for logic for detection of RWCU/SDC pipe break outside containment.

Plate-type flow orifices are used for flow monitoring, of demineralizer inlet flow, and to open the demineralizer bypass control valve if the flow exceeds the demineralizer capacity.

Safety Evaluation

The RWCU/SDC system functions are not safety-related with the exception of containment isolation functions, and providing instruments to detect high differential mass flow to detect

RWCU/SDC break outside the containment. Refer to Subsection 6.2.4 for containment isolation valves and Subsection 7.3.3 for containment isolation and break detection function by LD&IS.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the RWCU/SDC system and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the criteria in their order of listing in the table and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 50.55a (IEEE 279)

Addressing RG 1.153 and IEEE 603 below covers 10 CFR 50.55a.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Resolution of unresolved and generic safety issues for I&C is discussed in Subsection 7.1.2.2.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP 7.4 and with Table 7.1-1, the following GDC are addressed for shutdown systems:

- Criteria: GDC 2, 4, 13, 19, and 24.

  Conformance: The RWCU/SDC system is not a safety-related system for the ESBWR but is designed in conformance with the listed GDC.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.4, and with Table 7.1-1, there are no regulatory guides applicable to the nonsafety-related RWCU/SDC.

Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.4, and with Table 7.1-1, only BTP HICB-16 applies to the RWCU/SDC system.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

The level of detail provided herein for the RWCU/SDC System conforms to this BTP.

7.4.3.3 Testing and Inspection Requirements

The RWCU/SDC system instruments are calibrated and tested during the preoperational testing program to confirm the instrumentation is correctly installed and functions as designed. In

addition, calibration and surveillance testing of the containment isolation devices are performed at regular intervals in accordance with the plant Technical Specifications. Instrumentation requiring regular calibration, testing, and maintenance are mounted on accessible panels or racks located outside high radiation areas to the maximum extent possible.

7.4.3.4 Instrumentation Requirements

Operation of the RWCU/SDC system is from the main control room. The main instrumentation available to the control room operator includes the following:

- Manual and automatic flow controllers for system, demineralizer, and overboarding flow;
- Flow indication for system, demineralizer, and overboarding flow;
- Position indication for containment isolation valves, flow control valves, and all motor-operated valves;
- Temperature indication for demineralizer influent water;
- Conductivity recorder for demineralizer influent and effluent;
- Temperature for the system supply water (from the bottom RPV head);
- Temperature for the system return (to feedwater line) water;
- Temperature for the non-regenerative and regenerative heat exchangers' water (reactor water sides);
- Various process alarms (e.g., high water temperatures, high overboarding line pressure, low system flow, high system flow, high conductivity, etc.); and
- Pressure indication for the overboarding line.

7.4.4 Isolation Condenser System

7.4.4.1 Design Basis

Refer to Subsection 5.4.6.1.

7.4.4.2 System Description

Refer to Subsection 5.4.6.2.

7.4.4.3 Safety Evaluation

Compliance of Isolation Condenser System (ICS) equipment other than instrumentation and control is addressed in Subsection 5.4.6.3. Compliance of ICS instrumentation and control equipment is addressed in this subsection.

The ICS is designed to operate from safety-related power sources. The system instrumentation is powered by four divisionally separated sources of safety-related power. The ICS uses a two-out-of-four logic for automatic operation or isolation of each of the four separate isolation condenser (IC) trains as shown in Figure 7.4-3. The actuating logic and actuator power for the inner isolation valves for the four IC trains are on a different safety-related 250 VDC/120 VAC divisional power sources than that for the outer isolation valves. Interdivisional fiber optic

isolators are used to separate the four sensor inputs to the single divisional actuation logic circuits. An IC loop requires power from at least one of two safety-related divisional power source to automatically start, and each of the four IC loops is started using a different safety-related power sources. Consequently, the loss of one of the four safety-related power supplies will not result in the loss of any one IC train. However, a second source of safety-related power is provided to operate the IC automatic venting system during long-term IC operation; otherwise, the remote manually controlled backup venting system, which uses one of the divisional power sources that starts the IC, can be used for long-term operation.

If the four safety-related power supplies used to start the ICs fail, then the available ICs would automatically start because of the "fail open" actuation of the condensate return bypass valves on loss of electrical power to the solenoids which control these nitrogen-actuated valves. In addition, when both solenoids of any single IC train Condensate return bypass valves are de-energized, as in a loss of two divisions of electrical power supply, the accumulator path shall be closed and the nitrogen in the valve operator shall be vented, so that the spring opens the valve resulting in initiation of the affected IC trains

The IC System normally starts into operation automatically on high reactor pressure, low reactor water level (Level 2) with time delay, low reactor water level (Level 1.5), loss of power generation busses (same signal that initiates reactor scram), or on Main Steamline Isolation Valves (MSIVs) position indication (Indicating closure) whenever the reactor mode switch is in the RUN position. Signals which initiate closure of the MSIV are defined in detail in the section on the NBS and LD&IS. Each IC train can also be manually initiated as stated in section 7.4.4.5. The operator is able to stop any individual IC train whenever the RPV pressure is below a reset value, overriding IC automatic actuation signal coming from MSIV closure.

The residual heat removal function of the safety-related ICS is further backed up by the safety-related ESF combination of ADS, PCCS, and GDCS, or by the nonsafety-related RWCU/SDC loops or the make-up function of the CRD system operating in conjunction with safety relief valves and the suppression pool cooling systems.

Table 7.1-1 identifies the ICS and the associated codes and standards applied in accordance with the SRP. The following analysis lists the applicable criteria in their order of listing in the table and discusses the degree of conformance for each.

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: ICS complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. The ICS is divisionalized and redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail

  Conformance: The level of detail provided for the ICS within the Tier 1 and Tier 2 documents conforms to this BTP.

- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the Standard Review Plan for Section 7.4 and Table 7.1-1, the following GDC are addressed for the ICS:

Criteria: GDC 1, 2, 4, 13, 19 and 24.

Conformance: The ICS complies with these GDC.

Regulatory Guides (RGs)

In accordance with Table 7.1-1, the following RGs are addressed for the ICS:

RG 1.53 - Application of the Single-Failure to Nuclear Power Protection Systems - The ICS meets the requirements of RG 1.53.

RG 1.75 - Physical Independence of Electric Systems - Separation within the ICS is such that controls, equipment, and wiring are segregated into four separate safety-related logic groups.

RG 1.105 - Instrument Setpoints for Safety-Related Systems - The setpoints used to initiate ICS automatic operation or isolation are established consistent with this guide. NRC accepted Reference 7.2-1 provides the detailed description of this methodology.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems - The ICS complies with RG 1.118.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems - The ICS complies with this regulatory guide.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control System (SSLC), in Subsection 7.3.4, and in Subsection 7.1.2.2.

Branch Technical Positions (BTP)

In accordance with Table 7.1-1, the following BTPs are addressed for ICS:

BTP-HICB-11 - Guidance on Application and Qualification of Isolation Devices

SSLC logic controllers for ICS use fiber optic cables for interconnections between safety-related divisions for data exchange and for interconnections from safety-related to nonsafety-related devices.

BTP HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

ICS logic resides within the SSLC. The SSLC conforms to this BTP. Additional discussion is in Subsection 7.2.1.3.

BTP HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

This BTP does not apply to ICS nor SSLC. See Subsection 7.2.1.3 for additional discussion.

BTP HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

This BTP is applicable to all sections of the DCD including this section on ICS. This section content conforms to this BTP.

BTPs 14, 17, 18 and 21 are addressed in conjunction with the SSLC in Subsection 7.3.4.3.

7.4.4.4 Testing and Inspection Requirements.

Refer to Subsection 5.4.6.4.

7.4.4.5 Instrumentation Requirements.

Refer to Subsection 5.4.6.5.

Instruments

The following ICS indications are reported in the control room:

- Radiation level for each IC pool compartment airspace
- Mass flow rate in condensate return line
- Mass flow rate in steam supply line
- Temperature of steam and condensate return lines
- Temperature of IC top and bottom vent lines
- Valve position indication

The following manual controls are provided by the IC systems:

- Manual control to enable the operator to open/close condensate return valves
- Manual control to enable the operator to close condensate return isolation valves
- Manual control to enable the operator to close steam supply isolation valves

- Manual control to enable the operator to open/close all bottom vent valves
- Manual control to enable the operator to open/close all top vent valves
- Manual control to enable the operator to open/close purge line valve

7.4.5 COL Information

None.

7.4.6 References

None.

Table 7.4-1

Remote Shutdown System Interface

Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) System
The following RWCU/SDC equipment functions can be controlled from the remote shutdown panel. Equipment status indication is also provided on the remote shutdown panel, as indicated below:
1. Mid-vessel suction line valve [open/closed (o/c) status) A, B]
2. Mid-vessel suction line control valve (valve position) A, B
3. Bottom head suction line valve (o/c status) A, B (2 valves each)
4. Inboard suction line valve (o/c status) A, B
5. Outboard isolation valve (o/c status) A, B
6. Outboard isolation bypass line valve (o/c status) A, B
7. Regenerative heat exchanger tube-side bypass line valve (o/c status) A, B
8. Non-regenerative heat exchanger discharge valve (o/c status) A, B
9. Shutdown cooling discharge line control valve (valve position) A, B
10. Regenerative heat exchanger shell-side isolation valve (o/c status) A, B
11. RWCU/SDC return to feedwater line discharge valve (valve position) A, B
12. Pump adjustable speed drive (output frequency) A, B
The following RWCU/SDC instrumentation is provided for display on the remote shutdown panel:
1. Suction line flow A, B
2. Non-regenerative heat exchanger outlet temperature A, B
3. Pump discharge flow A, B

Table 7.4-1

Remote Shutdown System Interface

Control Rod Drive (CRD) System
The following CRD equipment functions can be controlled from the remote shutdown panel. Equipment status indication is also provided on the remote shutdown panel, as indicated below:
1. Pump suction filter bypass valve (o/c status) A, B
2. Pump discharge control valve (valve position) A, B
3. Condensate storage tank return test valve (o/c status)
4. Charging water line AO isolation valve (o/c status)
5. Purge water line AO isolation valve (o/c status)
6. Pump discharge test valve (o/c status)
7. Pump (on/off status) A, B
The following CRD instrumentation is provided for display on the remote shutdown panel:
1. Pump suction pressure indication A, B
2. Pump discharge flow indication A, B
Reactor Component Cooling Water (RCCW) System
The following RCCW equipment functions can be controlled from the remote shutdown panel. Equipment status indication is also provided on the remote shutdown panel, as indicated below:
1. RCCW heat exchanger inlet valve (o/c status) A, B
2. RCCW heat exchanger bypass valve (o/c status) A, B
3. Chiller inlet valve (o/c status) A, B
4. Drywell cooler inlet valve (o/c status) A, B
5. Drywell cooler outlet valve (o/c status) A, B
6. RWCU/SDC non-regenerative heat exchanger inlet valve (o/c status) A, B

Table 7.4-1

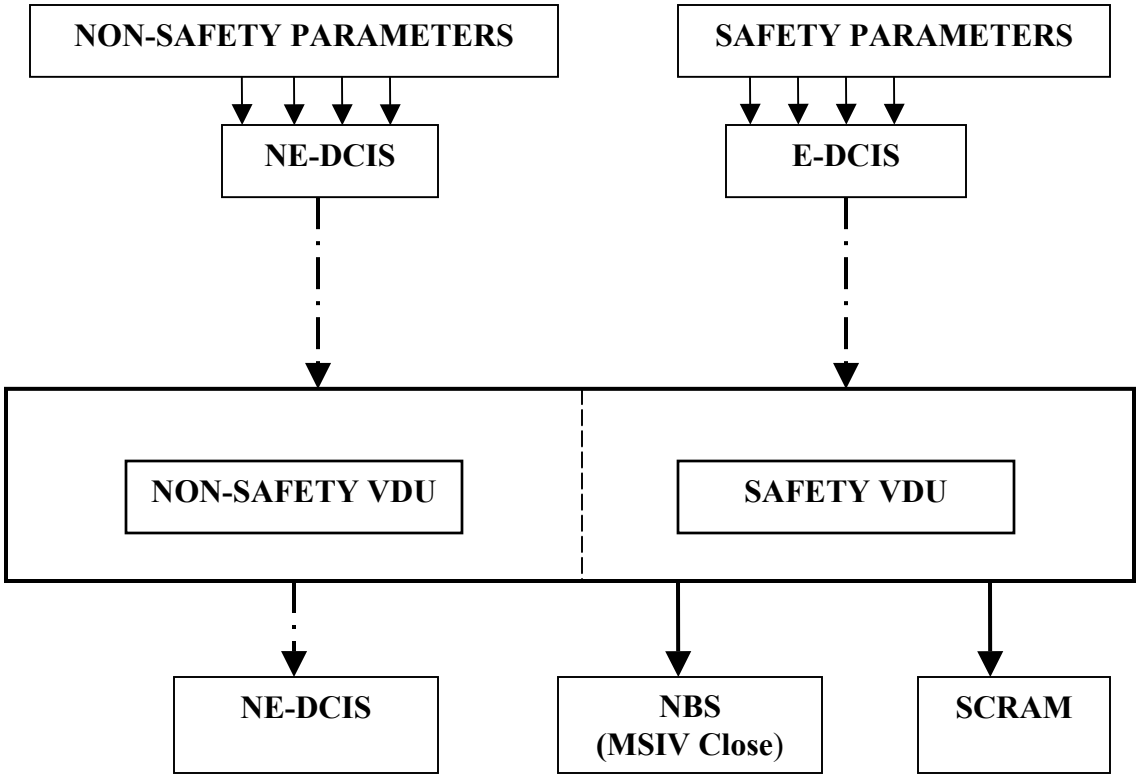
Remote Shutdown System Interface

7. FAPCS heat exchanger inlet valve (o/c status) A, B
8. RCCW pump discharge valve (o/c status) A, B, C, D
9. RCCW pump (on/off status) A, B, C, D
The following RCCW instrumentation is provided for display on the remote shutdown panel:
1. RCCW heat exchanger outlet temperature indication A, B
2. RCCW heat exchanger inlet flow indication A, B
Plant Service Water (PSW) System
The following PSW equipment functions can be controlled from the remote shutdown panel. Equipment status indication is also provided on the remote shutdown panel, as indicated below:
1. PSW pump discharge valve (o/c status) A, B, C, D
2. Turbine Component Cooling Water (TCCW) heat exchanger inlet valve (o/c status) A, B
3. TCCW heat exchanger outlet valve (o/c status) A, B
4. PSW pump (on/off status) A, B, C, D
The following PSW instrumentation is provided for display on the remote shutdown panel:
1. PSW discharge temperature indication A, B
2. PSW discharge flow indication A, B
Electrical Power Distribution System
All nonsafety Electrical Power Distribution System equipment functions can be controlled from the remote shutdown panel. This list is typical for both of the diesel-generator backed 6.9 kV buses (10A11 and 10A21) and the connected loads.
1. 1200A breaker from unit auxiliary switchgear to diesel generator bus 10A21
2. 1200A breaker from reserve transformer to diesel generator bus 10A21
3. Diesel generator breaker tie to 6.9 kV bus 10A21

Table 7.4-1

Remote Shutdown System Interface

4. 6.9kV diesel generator bus 10A21 breaker to 480V bus 10B219 and 10B220 (two breakers)
5. Breakers connecting bus 10B219 to M/Cs 10B2191 and 10B2192
6. Breakers connecting bus 10B220 to M/Cs 10B2201 and 10B2202
The following Electrical Power Distribution System instrumentation is provided for display on the remote shutdown panel:
1. 6.9 kV M/C voltmeters for monitoring voltage on buses 10A11 and 10A21.
2. Diesel generator run-stop indication 1AG01, 1BG01
Nuclear Boiler System (NBS)
At least the following NBS instrumentation is provided for display on the remote shutdown panel:
1. Reactor water level wide range indication A, B
2. Reactor pressure indication A, B



- **RWCU/SDC**
- **FAPCS INTO IC & SP COOLING**
- **INJECT HP CRD**
- **ETC**

Figure 7.4-1. Remote Shutdown System Simplified Functional Diagram
(one of two divisions)

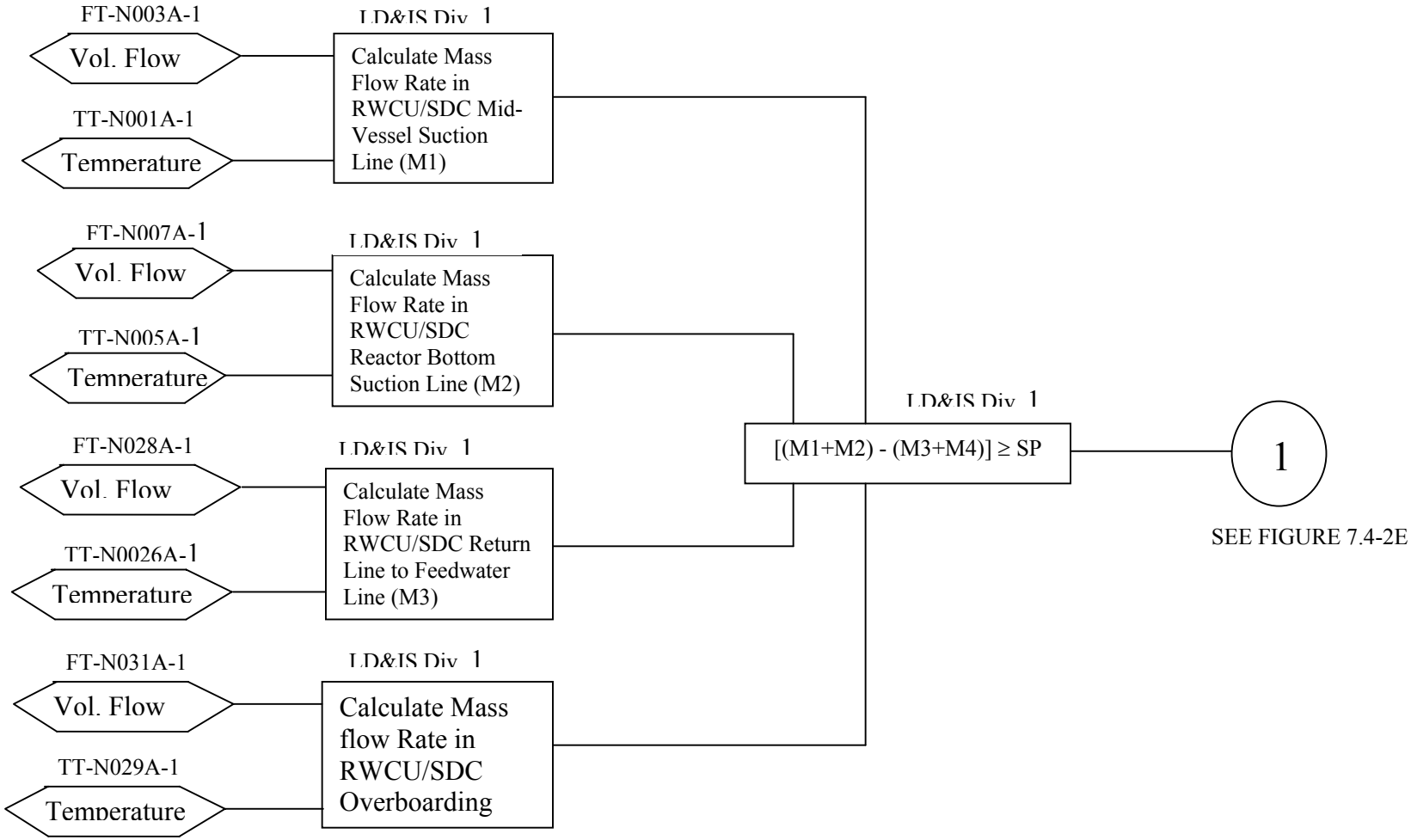


Figure 7.4-2A. RWCU/SDC System Train A Differential Mass Flow Logic- Division I
(Typical For Train B)

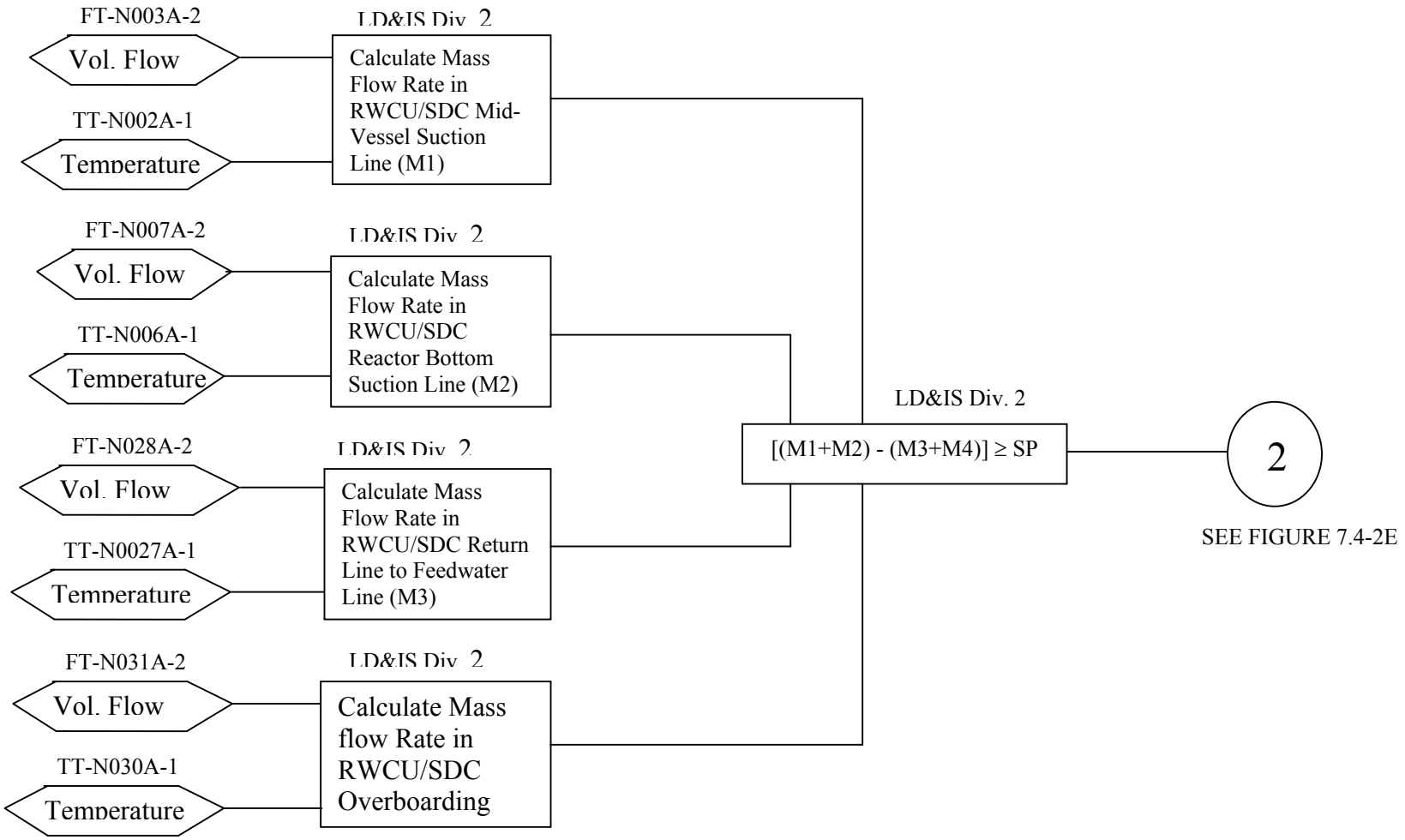


Figure 7.4-2B. RWCU/SDC System Train A Differential Mass Flow Logic- Division II
(Typical For Train B)

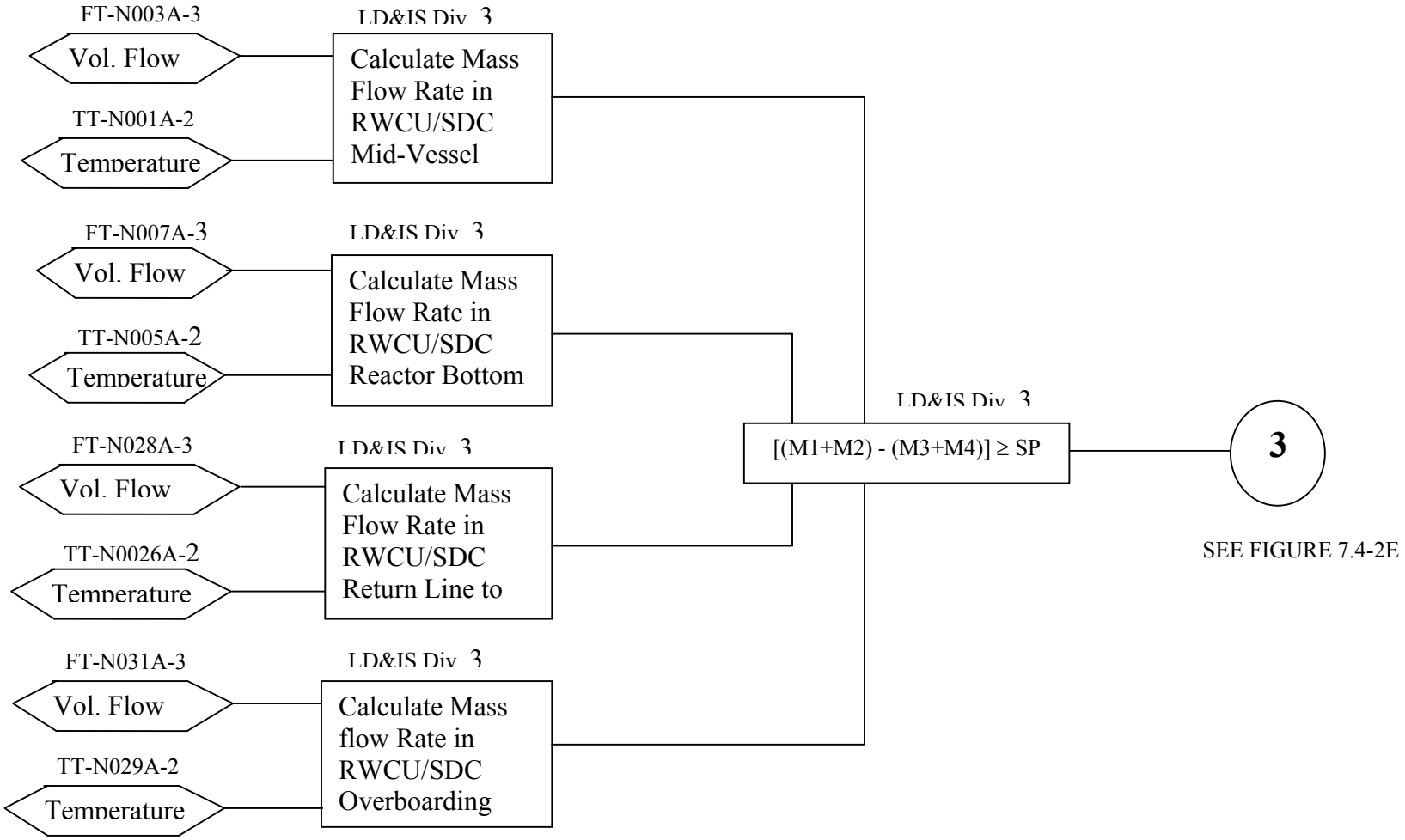


Figure 7.4-2C. RWCU/SDC System Train A Differential Mass Flow Logic- Division III
(Typical For Train B)

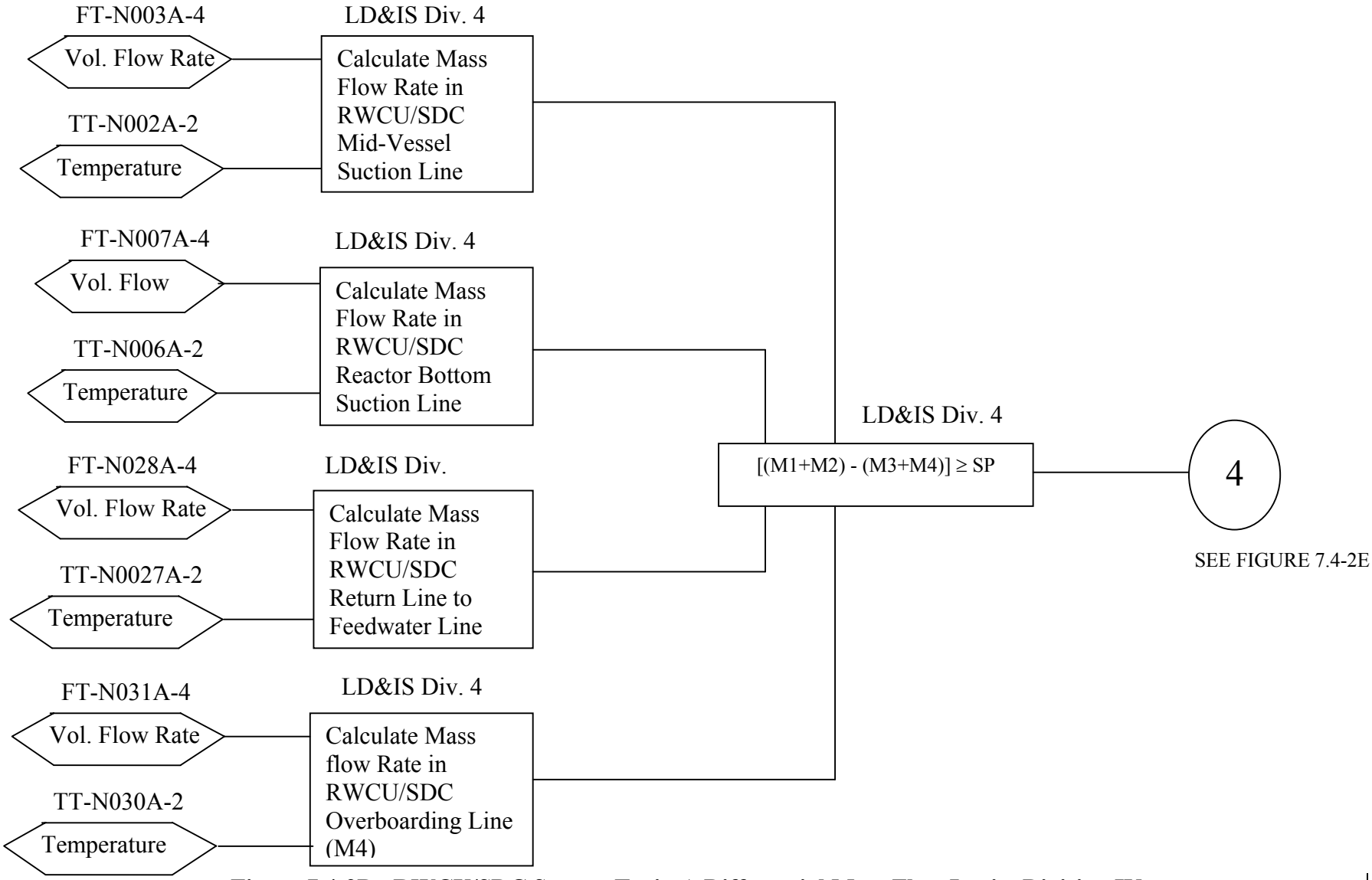


Figure 7.4-2D. RWCU/SDC System Train A Differential Mass Flow Logic- Division IV
(Typical For Train B)

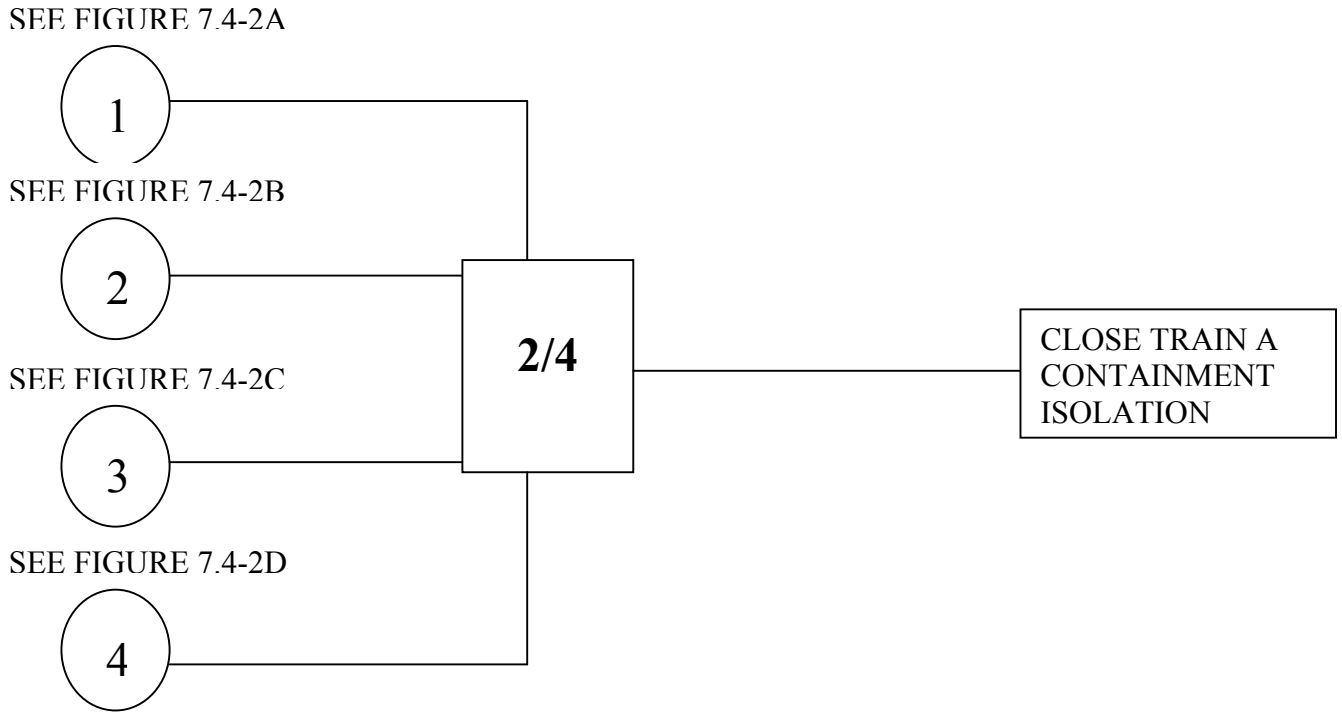


Figure 7.4-2E. RWCU/SDC Line Break Outside Containment Train A Isolation Logic
(Typical For Train B)

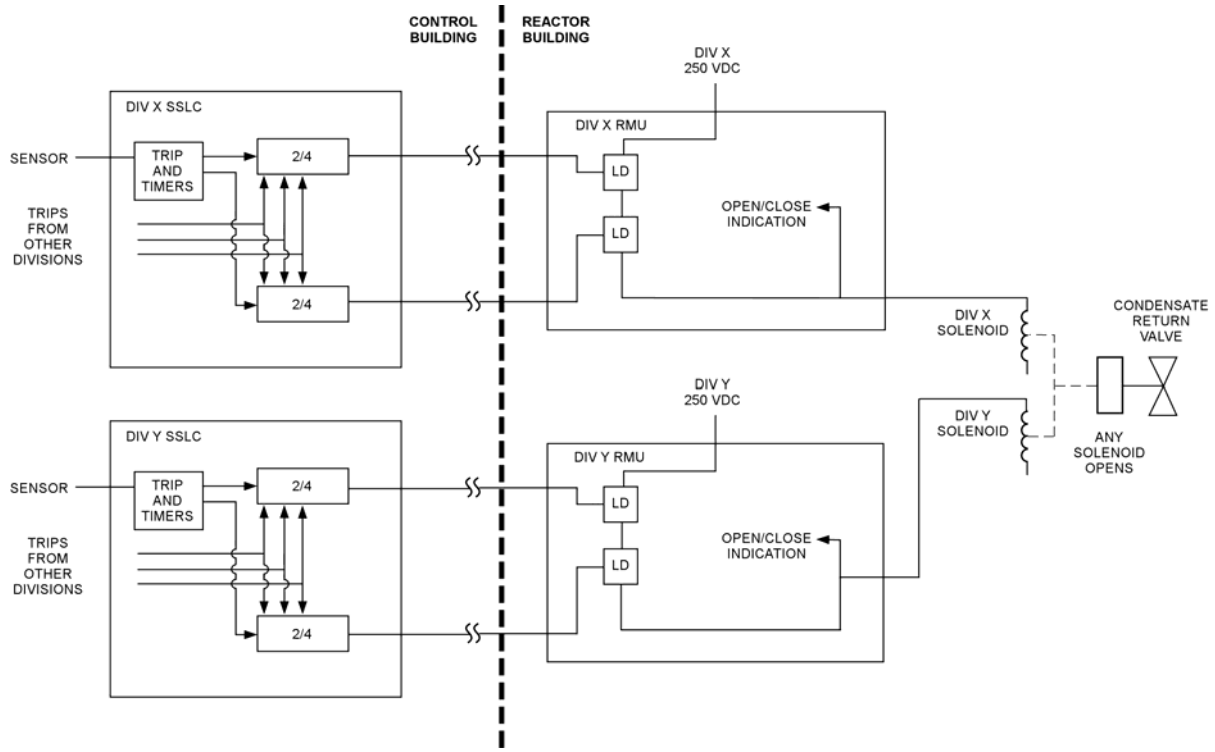


Figure 7.4-3. Isolation Condenser System Initiation and Actuation

7.5 SAFETY-RELATED AND NONSAFETY-RELATED INFORMATION SYSTEMS

7.5.1 General I&C Conformance to Regulatory Guide 1.97

7.5.1.1 System Descriptions

Safety-related display systems are those systems that provide information for the safe operation of the plant during normal operation, anticipated operational occurrences (AOOs) and accidents, to help ensure that manual safety-related functions are performed. The safety-related information systems include those systems that provide information (1) for manual initiation and control of safety-related systems, (2) to indicate that safety-related plant functions are being accomplished, and (3) to provide information, from which appropriate actions can be taken to mitigate the consequences of accidents. The Safety Parameter Display System, information systems associated with the emergency response facilities and nuclear data link, do not perform a safety-related function.

7.5.1.2 Post-Accident Monitoring System

Regulatory Guide (RG) 1.97 defines five "types" and three "categories" of plant variables for accident monitoring instrumentation. A discussion of these types and categories is provided below. Each variable has been defined as to both type and classification.

(1) Variable Types

Plant variables are divided into types according to the purpose of the indication to the plant operator. Any one variable may belong to more than one type.

(a) Type A - Type A variables are those variables that provide the primary information required to permit the control room operators to take the specified manual actions for which no automatic control is provided and that are required for safety-related systems to accomplish their safety functions for design basis accident events.

Primary information is information that is essential for the direct accomplishment of the specified safety function. Type A variables do not include those variables that are associated with contingency (or backup) action that may also be identified in written procedures or guidelines.

Type A variables are limited to those variables which are necessary (primary) to alert the control room operator of the need to perform pre-planned manual actions required for safety-related systems to perform their safety functions, such as maintaining Isolation Condenser System/Passive Containment Cooling System (IC/PCC) pool water. Variables that require actions specified by the Emergency Procedure Guidelines (EPGs) in response to specific limits have also been considered in performing the assessment documented in this chapter.

Type A variables do not necessarily include variables (1) that may indicate whether a specific safety function is being accomplished (Type B) or (2) that may indicate the need for contingency or corrective actions, resulting from the breach or potential breach of the plant barriers (Type C), or system(s) failure to respond correctly when needed (Type D), or (3) which may indicate to the operator that it is desirable to change or modify the operation/alignment of safety-related systems to maintain the plant in a safe condition after plant safety has been achieved.

(b) Type B - Type B variables are those variables that provide information to the control room operators to indicate whether plant safety functions are being accomplished, including controlling reactivity, cooling the core, maintaining reactor coolant system integrity, and maintaining containment integrity.

(c) Type C - Type C variables are those variables that provide information to the control room operators to indicate, (1) the extent to which parameters that could cause a breach in the containment have exceeded design basis values, or (2) that barriers to fission product release have the potential for being breached or have been breached. These barriers are the fuel cladding, primary coolant pressure boundary, and containment.

The ESBWR design features a Containment enclosed by Reactor Building.

The sources of potential breach are limited to the energy sources within the cladding, coolant boundary, or containment.

(d) Type D - Type D variables are those variables that provide information to the control room operators to indicate the successful operation of individual safety-related systems. The ESBWR does not contain an important to safety classification.

Type D variables provide information to permit the control room operators to ascertain the operating status of each individual safety-related system to the extent necessary to determine if each system is operating or can be placed in operation to help mitigate the consequences of an accident.

(e) Type E - Type E variables are those variables monitored to determine the magnitude of release of radioactive materials and to assess the continuation of such releases. These variables should permit the control room operators to monitor the effluent discharge paths and environs within the site boundary to ascertain if there have been significant releases (planned or unplanned) of radioactive materials and to continually assess such releases.

In particular, Type E variables monitor:

- The planned paths for effluent release;
- Plant areas inside buildings where access is required to service safety-related equipment; and
- On-site location where unplanned releases of radioactive materials may be detected.

(2) Categories of Variables

The design and qualification criteria for the instrumentation used to measure the various variables are divided into three categories that provide a graded approach to instrumentation criteria depending on importance to safety of the variables.

In general, Category 1 provides for full qualification, redundancy, and continuous real-time display and requires on-site (standby) power. Category 2 provides for qualification, but is less stringent in that it does not (of itself) include seismic qualification, redundancy, or continuous display and requires only a high-reliability power source (not necessarily standby power). Category 3 is the least stringent. It provides for high-quality commercial-grade equipment that requires only off-site power.

(a) Category 1 - Category 1 represents the most stringent criteria and is used for primary variables. Primary variables are those parameters that most directly indicate the accomplishment of a safety function. Type A variables are considered to be Category 1. For Types B and C, the primary variables are Category 1 while backup variables are generally Category 3.

(b) Category 2 - Category 2 provides less stringent criteria and generally applies to instrumentation designated for indication of system operating status. Most Type D variables are classified as Category 2.

(c) Category 3 - Category 3 provides criteria for high quality backup and diagnostic instrumentation or for other instrumentation where the state of the art does not support requirements for higher qualified instrumentation.

(3) Design and Qualification Criteria

The following design and qualification criteria for Category 1, 2, and 3 variables are detailed in RG 1.97:

- Equipment qualification;
- Redundancy;
- Power sources;
- Channel availability;
- Quality assurance;
- Display and recording;
- Range;
- Equipment Identification;
- Interfaces;
- Servicing, testing, and calibration;
- Human factors; and
- Direct measurement.

A detailed listing of the design and qualification criteria for Categories 1, 2 and 3 is provided in Table 7.5-1.

In addition to design and qualification criteria, Regulatory Guide 1.97 provides a comprehensive listing of "BWR variables" which addresses accident-monitoring requirements. Table 7.5-2 was developed using Table 2 of Regulatory Guide 1.97 as a guide. Design and qualification criteria are addressed as category designations in accordance with the discussion above. Variables listed Table 7.5-2 without comment meet the design and qualification requirements of Regulatory Guide 1.97; exceptions are noted in the comment column.

7.5.1.3 Systems Analysis - Post-Accident Monitoring System

(1) Type A Variables

Type A variables are fundamentally plant parameters needed to alert the control room operators to take safety actions by manually initiating a system or function which otherwise would not be automatically initiated in the course of an event. Regulatory Guide 1.97 does not specify Type A variables and the list of ESBWR Type A variables is based on a review of the ESBWR design.

The list of Type A variables is based on a review of accidents described in Chapter 15 and a review of the Emergency Procedure Guidelines (EPGs). The event descriptions of Chapter 15 were reviewed to determine the ESBWR plant safety-related systems that would require manual initiation and the associated primary variables. A summary of the Type A variables identified through this process is shown in Table 7.5-3. However, for ESBWR there are no instruments in this application. Details of the Type A variable assessment are provided below.

(a) Type A Variable Evaluation and Analysis - Chapter 15 contains discussions of numerous events, some of which are not design basis accidents.

Variables associated with normal operations are excluded from further investigation because those activities are planned actions that would not normally be expected to cause a threat to the general public.

The Chapter 15 events are considered in identifying the parameters used in the performance of the required operator actions.

The EPGs were also reviewed to determine if there were other variables not specifically identified by Chapter 15 that are associated with required operator actions. Some of these variables, especially those related to emergency action, are considered beyond the scope of the regulatory guide by virtue of requiring "contingency actions that are identified in written procedures."

The Reactor Building temperatures are excluded from the Type A variable list because they initiate automatic isolation of systems containing primary coolant on high area temperatures. Other Reactor Building area parameters (area water levels and radiation) were excluded because they represent early actions taken to limit the amount of plant effluent release to below those values used as a basis for the plant safety analysis. These parameters were considered to lead to contingency actions and thus are not required to be Type A.

The off-site release rate is excluded from the Type A Variable List because:

- The source terms required to reach release rates associated with a general emergency (the point at which the emergency action is required by the EPG) can only occur following a release of a substantial proportion of the fuel noble gas inventory. Prevention of such a release is a primary goal of the RPV control guideline and the emergency action (emergency depressurization) specified in the Radioactivity Release Control guidelines would have been previously initiated in response to other variables (e.g., RPV Water Level).
- The operator action (based on off-site release rate) to isolate lines discharging outside the containment and safety envelope are intended to be taken at levels low enough as to not pose a significant risk for the general public and, in addition, primary lines which

communicate with the RPV are automatically isolated. Other lines which pass outside of the containment and safety envelope, but which do not communicate directly with the RPV, also receive automatic isolation signals, which satisfies the intent of the EPG action for these lines.

Thus, response to the radioactivity release control guideline is considered to be a contingency action and is not required to be Type A.

(2) General Variable Assessments

This section summarizes the individual variable assessments concentrating on deviations identified between the design of the ESBWR and the need for unambiguous indication stated in Regulatory Guide 1.97.

Strict compliance with the regulatory guide is not provided. In some cases, an acceptable alternate (e.g., alternative variable or combinations of variables) has been proposed which meets the intent of meaningful post-accident indications. Another approach chosen is to take exception to the guide where a reasonable justification can be provided.

(a) Drywell Pressure - Requirements for monitoring of drywell pressure are specified for both narrow range and wide range (see Table 7.5-2 for required instrument ranges). The narrow range-monitoring requirement is satisfied by the four divisions of safety-related drywell pressure instruments that provide inputs to the initiation of the RPS and the Emergency Core Cooling System (ECCS). The requirement for unambiguous wide-range drywell pressure monitoring is satisfied with four channels of instrumentation that satisfy the specified instrument range.

(b) Wetwell Pressure - Requirements for monitoring of wetwell containment pressure specify the monitored range to be –34.32 kPaG to three times the design pressure for concrete containments. For ESBWR, 3 times the design pressure is about 931.6 kPaG. The ESBWR containment has a diaphragm safety device, which relieves wetwell atmosphere at about 617.8 kPaG. Therefore, it is not credible for containment pressure to achieve 931.6 kPaG. For this reason and for better resolution of measurements, the top of the instrument range for containment pressure is 689.4 kPaG. Two channels of instrumentation covering this full pressure range provide adequate Post Accident Monitoring (PAM) indication of containment pressure since any disagreement between the outputs of the two channels could be resolved by operator's reference to the drywell pressure indicators as discussed above.

(c) Coolant Level in the Reactor —The RPV water level is the primary variable indicating the availability of adequate core cooling. Indication of water level by the differential pressure method is considered acceptable (without diverse methods of sensing and indication) provided adequate redundancy for qualification of unambiguous indication is provided over the entire range of interest which extends from the bottom of the core support plate to the centerline of the main steam lines.

In the ESBWR design, the RPV water level wide range instruments and fuel zone instruments are utilized to provide this Post Accident Monitoring (PAM) indication. The four divisions of wide range instruments cover the range from above the core to the main steam lines. The four channels of fuel zone instruments cover the range from below the core to the top of the steam separator shroud.

Evaluation has concluded that four channels of fuel zone level instrumentation provide adequate post accident monitoring capability. Post-accident operator actions will be in accordance with detailed procedures developed based upon the Emergency Procedure Guidelines (EPG). Using the four divisions of WRL and fuel zone instruments, an unambiguous indication of vessel water level can be determined, despite a postulated failure of a single instrument channel or division, and the operator could safely continue the execution of appropriate accident investigation activities as defined by the EOPs. Capability is provided to record reactor vessel water level that meets normal post-accident recording requirements per 10 CFR 50.34(f)(2), Item xxiv)(II.K.3.23). The plant computer function of the ESBWR will typically record all plant variables acquired by the plant safety and non safety related RMU for approximately 18 – 24 months; these data are available for both operator trending and long term archiving.

(d) BWR Core Temperature - Regulatory Guide 1.97 requires BWR core temperature (thermocouples) as a diverse indication of adequate core cooling. BTP HICB-10, Table 1 states that this variable is not necessary for satisfying the guidelines identified in Regulatory Guide 1.97. General Electric and the BWR Owners' Group have taken exception to the Regulatory Guide for diverse indication based upon studies regarding the relationship between reactor water level and adequate core cooling. The USNRC stated in Reference 7.5-1 that, "Both tests and analyses have shown that maintaining the water level above the top of the active fuel is sufficient to assure adequate core cooling, provided the reactor is tripped. The EPGs are designed to give preference to covering the core with water to cool it." So, instrumentation other than RPV water level indication is not required to assure indication of adequate core cooling.

(e) Drywell Sump Level - As allowed by BTP HICB-10, Table 1 Category 3 instrumentation is acceptable for this parameter because:

- For small leaks, the instrumentation will not experience a harsh environment; it will be an early indication of a very small reactor coolant system leak/break for those events for which the drywell cooling system remains operable; and
- For larger leaks, the sump drain lines isolate due to the increase in drywell pressure; and
- Drywell pressure and temperature indication can be used to detect leakage into the drywell; and
- The instrumentation neither automatically initiates nor alerts the operator to initiates operation of a safety system in a post-accident situation.

(f) Containment Isolation Valve Position - The containment isolation valve position information provides indication to the operator regarding the successful completion of the containment isolation safety function. Consistent with 10 CFR 50, Appendix A, General Design Criteria 54, 55, 56 and 57, lines that penetrate the reactor containment are provided with varying degrees of redundant manual, check and automatically initiated isolation valves. Indication of the successful completion of the containment isolation safety function is provided by valve closed/not closed indicators for individual power operated valves.

This arrangement, which provides redundant isolation valves and independent indication of valve position, is considered sufficient to satisfy the intent of Regulatory Guide 1.97 without requiring the use of triplicate instrument channels. Per BTP HICB-10, Table 1 redundant position

indication for each active containment isolation valve is not necessary, because the valves are redundant.

(g) Suppression Pool Water Temperature - The ESBWR Suppression Pool Temperature Monitoring Subsystem (SPTM) design satisfies the Regulatory Guide 1.97 requirements regarding redundancy. The SPTM is composed of four separate and independent instrument divisions. Each division has multiple thermocouples that are spatially distributed around the suppression pool. With this configuration, the bulk average suppression pool temperature can be determined even in the event of the loss of an entire division of instrumentation because thermocouple sensors of each division are located in close proximity to those of the other divisions to facilitate direct comparison.

(h) Drywell Air Temperature - Multiple temperature sensors distributed throughout the drywell detect local area "hot-spots" and monitor the operability of the Drywell Cooling System. This drywell air temperature monitoring system is a redundant system that satisfies the Regulatory Guide 1.97 monitoring requirements for bulk average drywell air temperatures.

(i) Standby Liquid Control (SLC) system Flow/Pressure — SLC flow indication / measurement is not provided because of the passive nature of the system and the short operating time. Status of injection is provided by control room indication of accumulator pressure and accumulator solution level. Both of these parameters are direct and independent indicators of injection quantity given normal operation of the system. Because of the high rate of injection by this system, verification of injection is almost immediately available (< 30 sec) by observation of accumulator level. The verification can be confirmed by observation of accumulator pressure, also a direct measure of injection under conditions of normal, unfaulted system operation.

(j) Standby Energy - Because the ESBWR is designed with non-ac-powered ECCS, the standby energy source (e.g., diesel generators) is classified as a nonsafety-related system and Category 3 instrumentation is justified for PAM. Required safety-related system power is provided from on-site Class 1E divisional batteries.

(k) Drywell / Wetwell Hydrogen/Oxygen – The Containment Monitoring System (CMS) contains two independent and redundant drywell/wetwell oxygen and hydrogen concentration monitoring channels. Emergency response actions regarding these variables are consistently directed toward minimizing the magnitude of these parameters. This two-channel CMS design provides adequate PAM indication because, in the event that the two channels of information disagree, the operator can determine a correct and safe action based upon the higher of the two (in-range) indications.

Nonsafety-related commercial grade hydrogen monitors will be used to meet the criteria of Regulatory Guide 1.7 since they will comply with the Category 3 design and qualification criteria of Regulatory Guide 1.97 for monitors used as diagnostic or backup indicators. In addition, they will comply with the Category 2 power source design and qualification criteria as specified in Table 1 of Regulatory Guide 1.97.

Nonsafety-related oxygen monitors will be used and will meet the Category 2 design and qualification criteria of Regulatory Guide 1.97 for monitors designated for indicating system operating status.

(l) Containment Area Radiation – The Containment Monitoring System (CMS) contains two independent and redundant radiation-monitoring divisions that provide separate indication of drywell and wetwell radiation levels. Emergency response actions regarding this variable are consistently directed toward minimizing the magnitude of this parameter. This two-channel CMS design provides adequate PAM indication because, in the event that the two channels of information disagree, the operator can determine a correct and safe action based upon the higher of the two (in-range) indicators. These instruments are classified as nonsafety-related and as Category 3 instrumentation.

(m) Active ESF Systems - The following systems identified in Regulatory Guide1.97 do not exist in the ESBWR:

- RCIC
- HPCF/HPCS/HPCI
- Core Spray System
- Cooling Water to ESF Components
- Main Steam Line Isolation Valve Leakage Control System

(n) Nonsafety-related Systems - The following systems are not safety-related and, therefore, Category 3 instrumentation is justified for PAM:

- Fuel and Auxiliary Pool Cooling System
- Reactor Water Cleanup/Shutdown Cooling System (e.g., SDC flow, heat exchanger temperature)
- Reactor Component Cooling Water System (e.g., RCCW system flow and temperature to other system components)

7.5.2 Containment Monitoring System

The Containment Monitoring System (CMS) provides the instrumentation to monitor:

- The atmosphere in the containment for high gross gamma radiation levels
- Drywell and wetwell for oxygen and hydrogen
- The pressure of the drywell and wetwell
- The temperature of the suppression pool water (Subsection 7.2.3)
- The suppression pool water level
- Drywell/wetwell hydrogen/oxygen concentration
- Containment area radiation

These parameters are monitored during both normal reactor operations and post accident conditions to evaluate the integrity and safe conditions of the containment. Abnormal measurements and indications initiate alarms in the main control room.

7.5.2.1 System Design Bases

CMS design shall be in conformance with the following system design criteria:

- CMS is classified as safety related and Seismic Category 1, and conforms to the relevant codes and standards that are specified in Table 7.1-1 for this system.
- The non-safety H_2/O_2 subsystem of CMS shall be automatically initiated by a LOCA signal for post-accident monitoring of oxygen and hydrogen content in the containment.
- Two-divisions that are redundant but physically and electrically independent shall be provided for radiation monitoring and gas sampling.
- Each CMS radiation monitoring subsystem shall measure the gross gamma dosage levels in the drywell and in the wetwell and provide a continuous display in the main control room of dose rates from each area. The measurement range specified in Table 7.5-2 conforms to RG 1.97 range limits for post-accident monitoring.
- Each CMS gas sampling subsystem shall monitor the atmospheric oxygen and hydrogen contents in the drywell and in the wetwell and provide measurements in the main control room in percent volume for each of the sampled gases. Sampling from the drywell or the wetwell is initiated either manually or automatically.
- Main control room alarms shall be provided for indications of high radiation dose rates, inoperative radiation monitors, high oxygen levels, high hydrogen levels, and abnormal sampling for each subsystem.
- Each gas sampling rack shall be provided with its own gas calibration sources of known concentration levels to calibrate periodically the oxygen and hydrogen analyzers and sensors.

7.5.2.2 System Description

CMS is a divisionalized and segregated (safety/non safety redundancy) monitoring system comprised of various subsystems. The system design is configured as shown in Figure 7.5-1. The specific system features are as follows:

- Radiation monitoring and gas H_2/O_2 sampling is provided for the drywell and for the airspace above the suppression pool.
- Each radiation-monitoring channel utilizes one gamma-sensitive ion chamber and one digital log radiation monitor. Four channels are provided; two for the drywell and two for the suppression pool (wetwell) airspace.
- During Normal plant operation, both the radiation monitoring and gas sampling subsystems are operating. For post-accident monitoring, the gas sampling subsystem is automatically activated by the LOCA signal to alternate its sampling between the drywell and the wetwell. The area of sampling can be manually selected or sequentially controlled.
- Heat tracing is provided on the gas sampling lines for control of moisture and condensation.

- Two isolation valves are provided on each sample and return line that penetrates the containment. Each line has one manual inner valve and one remote-control outer valve.
- Each gas sampling analyzer has two redundant pumps. One is used during normal operation and the other is used for added capacity or backup.
- Separate oxygen and hydrogen gas sources are provided in each CMS sampling rack of known compositions for monitor calibration.
- CMS piping connections permit the Post Accident Sampling subsystem to extract a periodic gas sample for laboratory analysis.

7.5.2.3 Safety Evaluation

The CMS design, including the sensors and the instrumentation channels, are engineered into both safety-related and nonsafety-related subsystems and are environmentally and seismically qualified for continuous monitoring during reactor operation, and abnormal and accident plant conditions. The system design conforms to the System Design Bases and with the relevant codes and standards that are specified for this system in Table 7.1-1.

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: Containment Monitoring System complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. The Containment Monitoring System safety-related subsystems are divisionalized and are redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: Containment Monitoring System demonstrates compliance by being able to provide automatic indication of bypassed and operable status.

- 50.34(f)(2)(xvii)(II.F.1), Accident Monitoring Instrumentation

  Conformance: Containment Monitoring System complies with this requirement.

- 50.34(f)(2)(xix)(II.F.3), Instrumentation for Monitoring Plant Conditions Following Core Damage

  Conformance: Containment Monitoring System complies with this requirement.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail
- Conformance: The level of detail provided for the Containment Monitoring System within the Tier 1 and Tier 2 documents conforms to this BTP.
- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following GDC are addressed:

- Criteria: GDC 1, 2, 4, 13, 19, and 24.

  Conformance: The CMS complies with these GDC. The GDC are generically addressed in Subsection 3.1.2.

Staff Requirements Memorandum (SRM)

- SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

  Conformance: The CMS alarm system meets the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:

- Alarm points are sent via dual networks to redundant message processors on dual power supplies. The processors are dedicated and vastly underutilized as they only do alarm processing.
- The alarms are displayed, on multiple independent VDUs (dual power supplies on each).
- The alarm tiles are driven by redundant datalinks to the alarm tiles (dual power). The alarm tile processor is redundant.
- Each alarm tile has at least two LEDs of each color.
- The only thing that is not redundant is the horn and voice speaker. Test buttons are available to test the horn(s) and all the lights.
- There are no alarms requiring manually controlled actions for safety systems to accomplish their safety functions.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following RGs are addressed for the CMS:

- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
- RG 1.53 - Application of the Single Failure Criterion to Nuclear Power Protection Systems
- RG 1.75 - Physical Independence of Electrical Systems
- RG 1.105 – Setpoints for Safety-Related Instrumentation
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems

Conformance: The CMS conforms to all of the above listed Regulatory Guides with the assumption that the same interpretations and clarifications identified in Subsection 7.1.2.2 also apply to CMS. .

Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control (SSLC) system, Subsection 7.1.2.2.

Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.5, and with Table 7.1-1, the following BTP is addressed for Containment Monitoring System:

- HICB-11 – Guidance on Application and Qualification of Isolation Devices
- HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 – Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 – Guidance on Digital Computer Real-Time Performance

Conformance: The Containment Monitoring System complies with all the above HICBs. Discussion of HICBs 14, 17, 18, and 21 are addressed in conjunction with the SSLC system in Subsection 7.3.4.3.

TMI Action Plan Requirements:

In accordance with the SRP for 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3), 10 CFR 50.34(f)(2)(xvii) (II.F.1) and 10 CFR 50.34 (f)(2)(xix)(II.F.3) apply to the Containment Monitoring System. The CMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A.

7.5.2.4 Testing and Inspection Requirements

In-Service and Surveillance Testing - Inservice testing shall be performed periodically on each CMS subsystems to verify operability and to assure its ready status for post accident monitoring. Surveillance testing shall include instrument channel checks of the radiation and gas monitors, functional tests to verify equipment operability, sensor calibration and response tests, and leakage tests of the gas sampling lines.

Validation Test of the Calibrated Gas Sources - Tests shall be conducted on the gas calibration sources to verify equipment operability and to certify that the required gas concentration levels are within acceptable limits.

Specific Channel Calibration Checks - Each radiation-monitoring channel shall be checked and calibrated using a known gamma radiation source with predominant photon energies. Channel response shall be checked for proper measurement and display and for alarm initiation.

Each oxygen and hydrogen gas-sampling channel shall be checked for proper calibration and response at least two input gas levels per Table 7.5-4.

Sample Gas Leakage Tests - The gas leakage from the sampling lines and associated gas analyzer panel is specified in Table 7.5-4.

7.5.2.5 Instrumentation Requirements

Radiation Level Monitoring - Each compartment in the primary containment is monitored for gross gamma radiation levels by two-divisional channels. Table 7.5-2 identifies the range of measurement and display. Each channel consists of an ion chamber detector and a digital log radiation monitor, with trip circuits set for high radiation and low/INOP indications.

Oxygen/Hydrogen Concentration Monitoring - Two divisional racks for analysis and measurements sample the oxygen/hydrogen concentration levels in each compartment of the containment. The range of measurement of hydrogen and oxygen contents is displayed in percent by volume for the inerted containment. Separate gas indicators for measurement of oxygen and hydrogen contents are provided in the main control room for each CMS subsystem. Trip circuits for alarm initiation are set for high oxygen and hydrogen concentration levels and for abnormal sampling flow indication.

7.5.3 Process Radiation Monitoring System

The Process Radiation Monitoring System (PRMS) provides the instrumentation for radiological monitoring, sampling and analysis of identified process and effluents streams throughout the plant. The PRMS provides alerts of excessive radiation levels and initiates automatically the required protection action to isolate radioactivity releases to the environs. The following process

and effluent paths and/or areas represent some of the major areas monitored for excessive radiation levels (partial list):

- Main Steamline radiation;
- Reactor Building HVAC Exhaust;
- Isolation condenser pool vent discharge
- Control Room air intake;
- Drywell sump LCW and HCW discharge;
- Fuel Storage Building Main Area HVAC;
- Refueling Handling Area Air;
- Turbine Building Ventilation HVAC Exhaust;
- Turbine Compartment Area Exhaust;
- Offgas Pre Treatment;
- Offgas Post Treatment;
- Radwaste Building Ventilation Exhaust.

The system design is configured as shown in Figure 7.5-2. Design description of the PRMS together with detector and channel requirements are included in Section 11.5.

7.5.3.1 Safety Evaluation

The PRMS design, including the sensors and the instrumentation channels, are engineered into both safety-related and nonsafety-related subsystems and are environmentally and seismically qualified for continuous monitoring during reactor operation, and abnormal and accident plant conditions. The system design conforms to the System Design Bases and with the relevant codes and standards that are specified for this system in Table 7.1-1.

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: Process Radiation Monitoring System complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. The Process Radiation Monitoring System safety-related subsystems are divisionalized and are redundantly designed so that failure of any instrument will not interfere with the system operation. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: Process Radiation Monitoring System demonstrates compliance by being able to provide automatic indication of bypassed and inoperable status.

- 50.34(f)(2)(xvii)(II.F.1), Accident Monitoring Instrumentation

  Conformance: Process Radiation Monitoring System complies with this requirement.

- 50.34(f)(2)(xix)(II.F.3), Instrumentation for Monitoring Plant Conditions Following Core Damage

  Conformance: Process Radiation Monitoring System complies with this requirement.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail
- Conformance: The level of detail provided for the Process Radiation Monitoring System within the Tier 1 and Tier 2 documents conforms to this BTP.
- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following GDC are addressed:

- Criteria: GDC 1, 2, 4, 13, 19, and 24.

  Conformance: The PRMS are in compliance with these GDC. The GDC are generically addressed in Subsection 3.1.2.

Staff Requirements Memorandum (SRM)

- SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability

  Conformance: The PRMS alarm system meets the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant as follows:

- Alarm points are sent via dual networks to redundant message processors on dual power supplies. The processors are dedicated and vastly underutilized as they only do alarm processing.
- The alarms are displayed, on multiple independent VDUs (dual power supplies on each).

- The alarm tiles are driven by redundant data links to the alarm tiles (dual power). The alarm tile processor is redundant.
- Each alarm tile has at least two LEDs of each color.
- The only thing that is not redundant is the horn and voice speaker. Test buttons are available to test the horn(s) and all the lights.
- There are no alarms requiring manually controlled actions for safety systems to accomplish their safety functions.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following Regulatory Guides are addressed for the PRMS:

- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
- RG 1.53 - Application of the Single Failure Criterion to Nuclear Power Protection Systems
- RG 1.75 - Physical Independence of Electrical Systems
- RG 1.105 – Setpoints for Safety-Related Instrumentation
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems

Conformance: The PRMS conforms to all of the above listed Regulatory Guides with the assumption that the same interpretations and clarifications identified in Subsection 7.1.2.2 also apply to PRMS.

Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the SSLC system, Subsection 7.1.2.2.

Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.5, and with Table 7.1-1, the following BTP is addressed for Containment Monitoring System:

- HICB-11 – Guidance on Application and Qualification of Isolation Devices
- HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints
- HICB-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors
- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 – Guidance on Self-Test and Surveillance Test Provisions

- HICB-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 – Guidance on Digital Computer Real-Time Performance

Conformance: The Process Radiation Monitoring System complies with the above BTPs. Discussion of BTPs 14, 17, 18, and 21 are addressed in conjunction with the Safety System Logic and Control System (SSLC) in Subsections 7.3.4 and 7.1.2.2.

TMI Action Plan Requirements:

In accordance with the SRP for 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3), 10 CFR 50.34(f)(2)(xvii) (II.F.1) and 10 CFR 50.34 (f)(2)(xix)(II.F.3) apply to the Process Radiation Monitoring System. The PRMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A

7.5.4 Area Radiation Monitoring System

The primary function of the nonsafety-related Area Radiation Monitoring System (ARMS) is to continuously monitor the gamma radiation levels within the various areas of the plant and to provide an early warning that predetermined exposure rates are exceeded. The ARMS consists of various area radiation detectors located at accessible areas of the plant and utilizes local and control room alarms for immediate warning. The gross gamma radiation levels are monitored on a continuous basis, any change in exposure rates may be caused by operational transients or maintenance activities. Any high radiation levels are indicated by audible area alarms and control room alarms.

A functional block diagram of the ARMS is as shown in Figure 7.5-3. Design description of this system, together with detector locations, channel ranges, and alarm requirements are covered in Subsection 12.3.4.

7.5.4.1 Safety Evaluation

The ARMS design, including the sensors and the instrumentation channels, are engineered as a nonsafety-related system designed for continuous monitoring during reactor operation, and additionally during abnormal and accident plant conditions. The system design conforms to the System Design Bases and the relevant codes and standards specified in Table 7.1-1.

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: Area Radiation Monitoring System complies with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Since ARMS is a nonsafety-related system, therefore, this regulation is not applicable to this system. However, items covered in this regulation are covered by Containment Monitoring System.

- 50.34(f)(2)(xvii)(II.F.1), Accident Monitoring Instrumentation

  Conformance: Area Radiation Monitoring System complies with this requirement.

- 50.34(f)(2)(xix)(II.F.3), Instrumentation for Monitoring Plant Conditions Following Core Damage

  Conformance: Area Radiation Monitoring System complies with this requirement.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.5, and with Table 7.1-1, the following GDC are addressed:

- Criteria: GDC 2, 4, 13, 19, and 24.

  Conformance: The ARMS are in compliance with these GDC. The GDC are generically addressed in Subsection 3.1.2.

Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.5, and with Table 7.1-1, the following BTP is addressed for Area Radiation Monitoring System:

- HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

  Conformance: The level of detail in the Tier 1 and Tier 2 documents for the Area Radiation Monitoring System complies with the above BTP.

TMI Action Plan Requirements:

In accordance with the SRP for 7.5 and with Table 7.1-1, 10 CFR 50.34(f)(2)(xvii) (II.F.1) and 10 CFR 50.34(f)(2)(xix) (II.F.3) apply to the Area Radiation Monitoring System. The ARMS complies with these requirements, as indicated above. However, TMI action plan requirements are generically addressed in Appendix 1A

7.5.5 Pool Monitoring Subsystems

7.5.5.1 General Functional Requirements Conformance

Instrumentation is provided for automatic reactor scram or automatic suppression pool cooling initiation. Visual indication of pool temperature is continuously provided for operator awareness under all operating and accident conditions. The system is automatically initiated and

continuously monitors pool temperatures during reactor operation. This is discussed in Subsection 7.2.3.

7.5.5.2 Suppression Pool

The Containment Monitoring System is provided with temperature and water level instruments for monitoring suppression pool water temperature and water level, respectively. The temperature instrument generates a high water temperature signal when the suppression pool water temperature exceeds a high temperature limit. The suppression pool cooling mode of FAPCS is automatically initiated by the high pool temperature signal. The water level signal generates a low water level signal when the suppression pool low level decreases to below a low level setpoint. The signal trips the FAPCS pump when it operates with suction from the suppression pool.

These instruments provide functions necessary to maintain suppression water temperature and level required for the safety-related ECCS function. For this reason, they are classified as safety-related, and thus are required to meet the requirements for Category 1 component per Reg. Guide 1.97.

7.5.5.3 GDCS Pools

Gravity Driven Cooling System (GDCS) pools are provided with instruments for monitoring water level in these pools. The instrument generates a high or low water level signal when its water level reading increases above or decreases below the setpoints. The high and low level signal initiates an alarm in the MCR. Additionally the low level trips the FAPCS system pump operating in the GDCS pool cooling mode. The high level setpoint is established to avoid overflow of GDCS pool water. The low water level setpoint is established to prevent inadvertent draining of the pool water below the minimum level for the safety function.

These instruments provide necessary information to the operator for maintaining GDC water level required for the safety-related ECCS function. For this reason, they are classified as safety-related, and thus are required to meet the requirements for Category 1 components per Reg. Guide 1.97.

7.5.5.4 IC/PCC Pools

Isolation Condenser and Passive Containment Cooling System (IC/PCCS) pools are provided with instruments for monitoring water level in these pools. Each instrument generates a high or low water level signal when its water level reading increases above or decreases below the setpoints. The high or low level signal initiates an alarm in the MCR. Additionally, the low level signal trips the FAPCS system pump operating in the IC/PCCS pool cooling mode. The high level setpoint is established to avoid overflow of IC/PCCS pool water. The low water level setpoint is established to prevent inadvertent draining of the pool water below the minimum level for safety function.

These instruments provide necessary information to the operator for refilling the IC/PCCS pools following an accident. For this reason, it is classified as a safety-related component, and thus is required to meet the requirements for Category 1 components per Reg. Guide 1.97.

7.5.5.5 Spent Fuel Pool

The skimmer surge tanks are used for receiving overflow water from the spent fuel pool and as a suction source during the spent fuel pool cooling mode of operation. These tanks are provided with instruments for monitoring water level in the tanks. These instruments generate high, low and low-low water level signals when the water level reading exceeds their setpoints. These signals initiate high and low water level alarms in the MCR. Additionally, the low level signal is used for tripping the FAPCS C/C train pump operating in the spent fuel pool cooling mode. The high level setpoint is established to avoid overflow of skimmer surge tank water. The low water level setpoint is established to prevent inadvertent draining of the tank water below the minimum level for safety function.

These instruments provide necessary information to the operator for performing a safety-related function of refilling the spent fuel pool following an accident. For this reason, it is classified as a safety-related component and is required to meet the requirements for Category 1 components per Reg. Guide 1.97.

7.5.6 Wetwell-to-Drywell Vacuum Breaker Monitoring

The wetwell-to-drywell vacuum breakers are provided with four safety-related proximity sensors in four safety-related instrument divisions to monitor their closed position. See Subsection 6.2.1 for further discussion.

7.5.7 COL Information

None.

7.5.8 References

7.5-1 A. Thadani, USNRC, to D. Grace, Chairman BWR Owners' Group, letter "Safety Evaluation of BWR Owners' Group — Emergency Procedure Guidelines, Revision 4, NEDO-31331, March 1987," dated September 12 1988.

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
1. Equipment Qualification		
The instrumentation is qualified in accordance with Regulatory Guide 1.89, Qualification of Class IE Equipment for Nuclear Power Plants, and the methodology described in NUREG-0588, Interim Staff Position on Environmental Qualification of Safety-Related Electrical Equipment.	Same as Category 1	No specific provision
(For equipment located in a mild environment, no specific environmental qualification is required except as required by General Design Criterion 4 of 10 CFR 50.)	Same as Category 1	No specific provision
Instrumentation whose ranges are required to extend beyond those ranges calculated in the most severe design basis accident event for a given variable are qualified using the guidance provided in Paragraph 6.3.6 of ANS-4.5.	Same as Category 1	No specific provision
Qualification applies to the complete instrumentation channel from sensor to display where the display is a direct-indicating meter or recording device. If the instrumentation channel signal is used in a computer-based display, recording, or diagnostic program, qualification applies from the sensor up to and including the channel isolation device.	Same as Category 1	No specific provision
The seismic portion of qualification is in accordance with Regulatory Guide 1.100, "Seismic Qualification of Electric Equipment for Nuclear Power Plants." Instrumentation should continue to read within the required accuracy following, but not necessarily during, a safe shutdown earthquake.	No specific provision	No specific provision

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
2. Redundancy		
No single failure within either the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources concurrent with the failures that are a condition or result of a specific accident should prevent the operators from being presented the information necessary for them to determine the safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident. Where failure of one accident-monitoring channel results in information ambiguity (that is, the redundant displays disagree) that could lead operators to defeat or fail to accomplish a required safety function, additional information should be provided to allow the operators to deduce the actual conditions in the plant. This is accomplished by providing additional independent channels of information of the same variable (addition of an identical channel) or by providing an independent channel to monitor a different variable that bears a known relationship to the multiple channels (addition of a diverse channel). Redundant or diverse channels are electrically independent and physically separated from each other and from equipment not classified safety-related in accordance with Regulatory Guide 1.75, "Physical Independence of Electric Systems," up to and including any isolation device. Within each redundant division of a safety system, redundant monitoring channels are not needed.	No specific provision	No specific provision

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
3. Power Source		
The instrumentation is energized from a on-site (standby) power source, not necessarily standby power, and backed up by batteries where momentary interruption is not tolerable.	The instrumentation is energized from a high-reliability power source, not necessarily standby power, and backed up by batteries where momentary interruption is not tolerable.	No specific provision
4. Channel Availability		
The instrumentation channel is available prior to an accident except as provided in paragraph 4.11, "Exception," as defined in IEEE Std 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations," or as specified in the technical specifications.	The out-of-service interval is based on normal technical specification requirements on out-of-service for the system it serves, where applicable, or where specified by other requirements.	No specific provision
5. Quality Assurance		
The recommendations of the following Regulatory Guides pertaining to quality assurance are followed:	Same as Category 1 as modified by the following:	The instrumentation is of high-quality commercial grade and is selected to withstand the specified service environment.

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
Regulatory Guide 1.28, "Quality Assurance Program Requirements Design and Construction" Regulatory Guide 1.30 (Safety Guide 30), "Quality Assurance Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment"	Because some instrumentation is less important to safety than other instrumentation, the application of the same quality level is not necessary. The quality assurance requirements that are implemented provide control over activities affecting quality to an extent consistent with the importance to safety of the instrumentation	
Regulatory Guide 1.38, "Quality Assurance Requirements for Packaging, Shipping Receiving, Storage and Handling of Items for Water-Cooled Nuclear Power Plants"		
Regulatory Guide 1.58, "Qualification of Nuclear Power Plant Inspection, Examination, and Testing Personnel"		
Regulatory Guide 1.64, "Quality Assurance Requirements for the Design of Nuclear Power Plants"		
Regulatory Guide 1.74, "Quality Assurance Terms and Definitions"		
Regulatory Guide 1.88, "Collection, Storage, and Maintenance of Nuclear Power Plant Quality Assurance Records"		

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
Regulatory Guide 1.123, "Quality Assurance Requirements for Control of Procurement of Items and Services for Nuclear Power Plants"		
Regulatory Guide 1.144, "Auditing of Quality Assurance Programs for Nuclear Power Plants"		
Regulatory Guide 1.146, "Qualification of Quality Assurance Program Audit Personnel for Nuclear Power Plants"		
6. Display and Recording		
Continuous real-time display is provided. The indication is on a dial, digital display, CRT, or strip-chart recorder.	The instrumentation signal may be displayed on an individual instrument or it may be processed for display on demand.	Same as Category 2
Recording of instrumentation readout information is provided for at least one redundant channel.	Signals from effluent radioactivity monitors and area monitors are recorded.	Signals from effluent radioactivity monitors, and meteorology monitors are recorded.

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
If direct and immediate trend or transient information is essential for operator information or action, the recording is continuously available on redundant dedicated recorders. Otherwise, it may be continuously updated, stored in computer memory, and displayed on demand. Intermittent displays such as data loggers and scanning recorders may be used if no significant transient response information is likely to be lost by such devices.	Same as Category 1	Same as Category 1
7. Range		
If two or more instruments are needed to cover a particular range, overlapping of instrument span is provided. If the required range of monitoring instrumentation results in a loss of instrumentation sensitivity in the normal operating range, separate instruments are used.		
8. Equipment Identification (Also see item 11)		
Types A, B, and C instruments designated as Categories 1 and 2 are specifically identified with a common designation on the control panels so that the operator can easily discern that they are intended for use under accident conditions.	Same as Category 1	No specific provision
9. Interfaces		
The transmission of signals for other use is through isolation devices that are designated as part of the monitoring instrumentation and that meet the provisions of this document.	Same as Category 1	No specific provision

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
10. Servicing, Testing, and Calibration		
Servicing, testing, and calibration programs are specified to maintain the capability of the monitoring instrumentation. If the required interval between testing is less than the normal time interval between plant shutdowns, a capability for testing during power operation is provided.	Same as Category 1	Same as Category 1
Whenever means for removing channels from service are included in the design, the design facilitates administrative control of the access to such removal means.	Same as Category 1	Same as Category 1
The design facilitates administrative control of the access to setpoint adjustments, module calibration adjustments, and test points.	Same as Category 1	Same as Category 1
Periodic checking, testing, calibration, and calibration verification are in accordance with the applicable portions of Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems," pertaining to testing of instrument channels. (Note: Response time testing not usually needed.)	Same as Category 1	Same as Category 1
The location of the isolation device is such that it would be accessible for maintenance during accident conditions.	Same as Category 1	No specific provision
11. Human Factors (Also see item 8)		
The instrumentation is designed to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules.	Same as Category 1	Same as Category 1

Table 7.5-1

Design and Qualification for Instrumentation

Category 1	Category 2	Category 3
The monitoring instrumentation design minimizes the development of conditions that would cause meters, annunciators, recorders, alarms, etc., to give anomalous indications potentially confusing to the operator. Human factors analysis is used in determining type and location of displays (Chapter 18).	Same as Category 1	Same as Category 1
To the extent practicable, the same instruments are used for accident monitoring as are used for the normal operations of the plant to enable the operators to use, during accident situations, instruments with which they are most familiar.	Same as Category 1	Same as Category 1
12. Direct Measurement		
To the extent practicable, monitoring instrumentation inputs are from sensors that directly measure the desired variables. An indirect measurement is made only when it can be shown by analysis to provide unambiguous information.	Same as Category 1	Same as Category 1

Table 7.5-2

PAM Variable List

Variable	Range	Type	Category
Neutron Flux	1E-06% to full power	B	1
Control Rod Position	Full in or not full in	B	3
Boron Concentration	0 to 2000 ppm	B	3
Standby Liquid Control System Pressure	0 to 110% design pressure	D	2
SLC System Accumulator Solution Level	Top to bottom	D	2
BWR Core Temperature	200°F to 2300°F		
Reactor Coolant System Pressure	0 to 10.34 MPa (gauge) (1500 psig)	B,C,D	1
Isolation Condenser/Passive Containment Cooling System Pool Water Level	Below low water level to above overboarding line to suppression pool	D	2
Isolation Condenser Steam Line Differential Pressure (flow)	0 to 110% flow	C,D	2
Isolation Condenser Condensate Line Differential Pressure (flow)	0 to 110% flow	C,D	2
Isolation Condenser Valve Positions	Open or Closed	D	2
Isolation Condenser Pool Radiation	1E-07 to 1E-03 Gy/h (1E-02 to 1E+02 mR/hr	C,D, E	2
Coolant Level in Reactor	Bottom of core support plate to centerline of the main steam line	B	1
Gravity Driven Cooling System Pool Water Level	Below GDCS suction strainer to above high water level	D	2

Table 7.5-2

PAM Variable List

Variable	Range	Type	Category
Gravity Driven Cooling System Valve Positions	Closed - Not Closed	D	3
Suppression Pool Water Level	Bottom of Pool to 1.5m (5 ft) above normal water line	C,D	1
Suppression Pool Water Temperature	4 to 110°C (40 to 230°F)	D	2
Suppression Pool Valve Positions	Closed - Not Closed	D	1
Feedwater Flow	0 to 150% design flow	D	3
Condensate Storage Tank Level	Top to bottom	D	3
Standby Energy Status	Plant Specific	D	2
RWCU/Shutdown Cooling System Flow	0 to 110% design flow	D	3
RWCU/SDC System Non-Regen Heat Exchanger Outlet Temperature	4 to 177°C (40 to 350°F)	D	2
FAPCS Heat Exchanger Outlet Temperature	4 to 177°C (40 to 350°F)	D	2
Reactor Component Cooling Water System Flow	0 to 110% design flow	D	2
Reactor Component Cooling Water System Temperature to Components	4 to 93°C (40 to 200°F)	D	2
Wetwell Pressure	-34.5 kPa (gauge) (-5 psig) to 3 times design	B,C	1
Drywell Pressure	-34.5 to 20.7 kPa (gauge) (-5 to 3 psig) (narrow range), 0 to 110% of design pressure (wide range)	B,C,D	1
Drywell Air Temperature	4 to 227°C (40 to 440°F)	D	2

Table 7.5-2

PAM Variable List

Variable	Range	Type	Category
Drywell Water Level	Bottom of Drywell to Main Steamline	D	2
Drywell Sump Level	Top to Bottom	B,C	3
Containment Isolation Valve Positions	Closed - Not Closed	B	1
Drywell/Wetwell Hydrogen Concentration	0 to 30 Vol%	C	3
Drywell/Wetwell Oxygen Concentration	0 to 10 Vol%	C	2
Containment Area Radiation	1E-02 to 1E+05 Gy/hr (1 to 1E+07 R/hr)	C,E	1
Drywell Spray Flow	0 to 110% design flow	D	3
Emergency Ventilation Damper Position	Open - Closed Status	D	2
Primary Coolant (Gamma Spectrum)	3.7E+08 to 3.7E+14 Bq/l (10 μCi/ml to 10 Ci/ml) or TID-14844 Source Term in Coolant Volume	C	3
Coolant Radiation	1/2 Tech Spec limit to 100 times Tech Spec limit	C	1
High Radioactivity Liquid Tank Level	Top to Bottom	D	3
Containment Effluent Radioactivity - Noble Gas	3.7E+01 to 3.7E+10 Bq/l (1E-06 to 1E-02 μCi/cc)	C	3
Reactor Building (outside containment) Airspace (effluent) Radiation Noble Gas	3.7E+01 to 3.7E+10 Bq/l (1E-06 to 1E+03 μCi/cc)	C	2
Reactor Building Area Radiation	1E-03 to 1E+02 Gy/h (1E-01 to 1E+04 R/h	E	2

Table 7.5-2

PAM Variable List

Variable	Range	Type	Category
Service Area Radiation Exposure Rate	1E-03 to 1E+02 Gy/h (1E-01 to 1E+04 R/h	E	3
Purge Flows - Noble Gases	3.7E+01 to 3.7E+12 Bq/l (1E-06 to 1E+05 μCi/cc); 0 to 110% Vent Design Flow	E	2
Identified Release Points - Particulates and Halogens	3.7E-04 to 3.7E+09 Bq/l (1E-03 to 1E+02 μCi/cc); 0 to 110% Vent Design Flow	E	2
Airborne Radiohalogens and Particulates	3.7E-02 to 3.7E+04 Bq/l (1E-09 to 1E-03 μCi/cc)	E	3
Plant and Environs Radiation	1E-05 to 1E+02 Gy/h (1E-03 to 1E+04 R/h), photons; 1E-05 to 1E+02 Gy/h (1E-03 to 1E+04 R/h), beta and low energy photons	E	3
Plant and Environs Radioactivity	(Isotopic Analysis)	E	3
Meteorological Data (Wind Speed, Wind Direction, and Atmospheric Stability)	Refer to Regulatory Guide 1.97	E	3
On-Site Analysis Capability (Primary Coolant, Sump and Containment Air Grab Sampling)	Refer to Regulatory Guide 1.97	E	3

Table 7.5-3

Type A Variables

For ESBWR, there are no instruments in this application.

Table 7.5-4

CMS Testing and Inspection Requirements

Specified Channel Calibration – Each oxygen and hydrogen gas sampling channel	0 gas concentration and nominal level from 2 to 5% from calibrated sources
Sample Gas Leakage Test – Sample lines and associated gas analyzer panel	Less than 0.01cc/sec at peak sample pressure

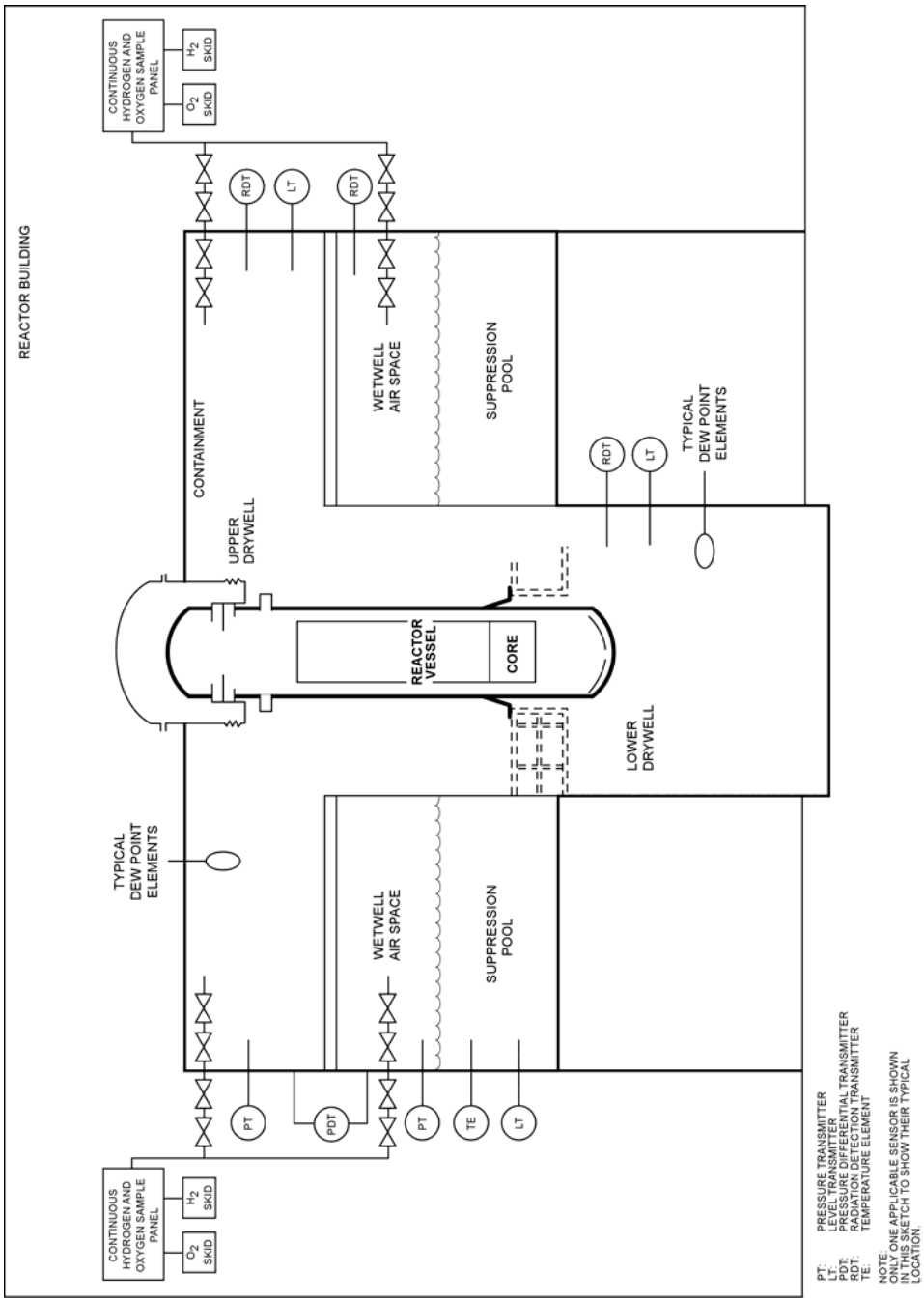


Figure 7.5-1. Containment Monitoring System Design

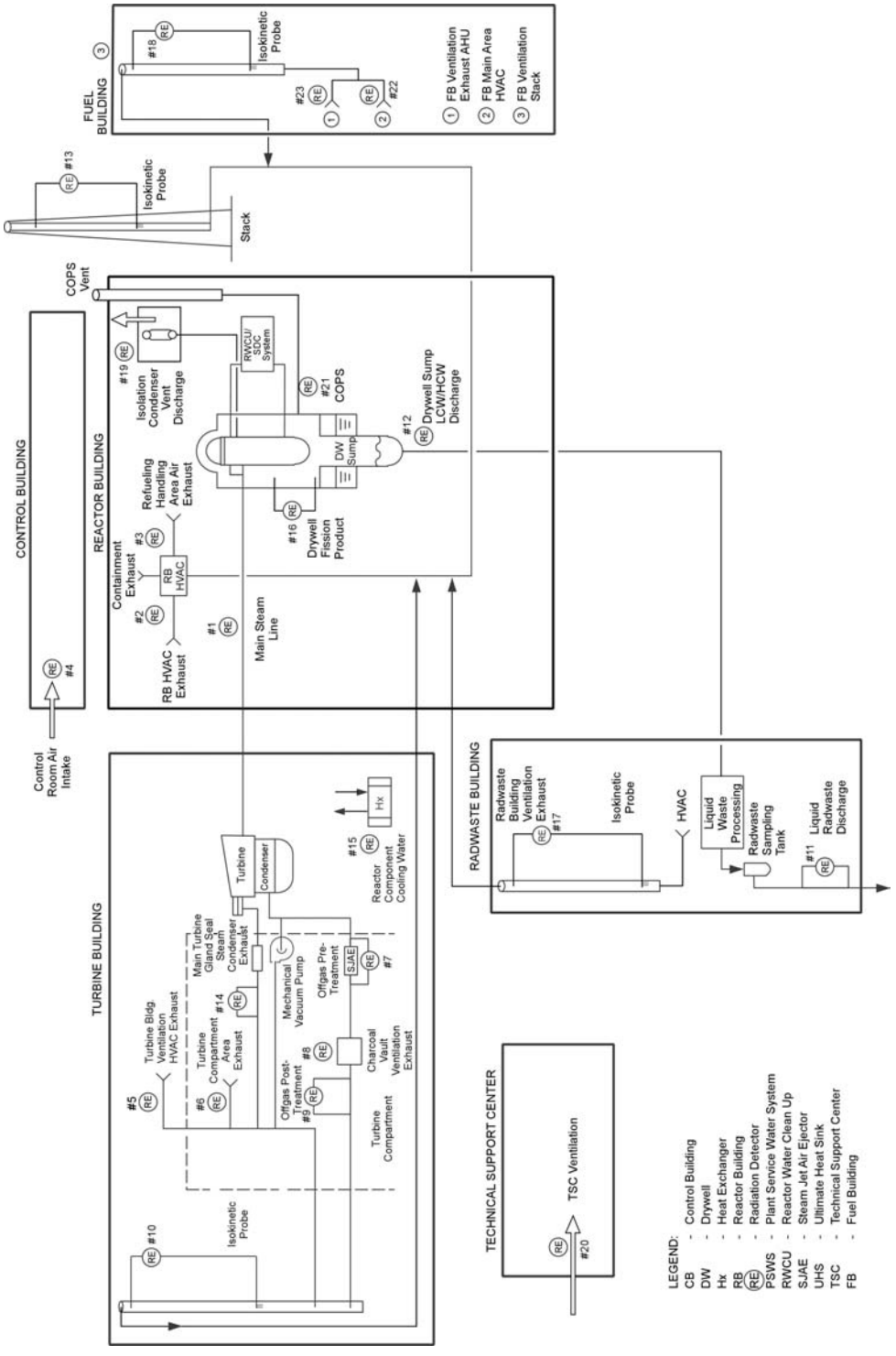


Figure 7.5-2. Process Radiation Monitoring System Design

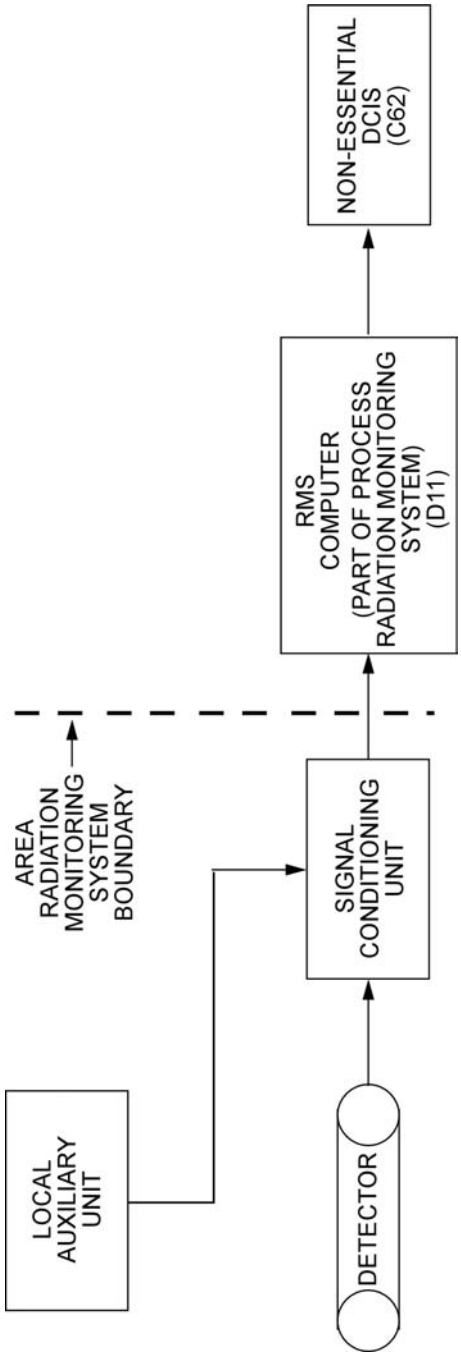


Figure 7.5-3. Area Radiation Monitoring System Functional Block Diagram

7.6 INTERLOCK SYSTEMS

In accordance with the Standard Review Plan (SRP), the systems addressed in this section are "those interlock systems important to safety which operate to reduce the probability of occurrence of specific events or to maintain safety systems in a state to assure their availability in an accident." This is further clarified to include two types of interlock functions: (1) high pressure/low pressure (HP/LP) interlocks to prevent over-pressurization of low pressure systems which are connected to high pressure systems, and (2) interlocks to isolate safety-related systems from nonsafety-related systems. Both types of functions are addressed herein.

7.6.1 HP/LP System Interlock Function

7.6.1.1 Design Bases

Fuel and Auxiliary Pools Cooling System (FAPCS) is a low pressure piping system. Its low pressure coolant injection (LPCI) line is connected to the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) Loop B discharge line, which is connected to the reactor vessel via the Feedwater Loop A discharge line.

During reactor power operation, the high pressure condition in the RWCU/SDC system piping exceeds the design pressure of the low pressure FAPCS piping. This subsection discusses the reactor pressure interlock design provided to prevent over-pressurization of the FAPCS piping. The FAPCS design is discussed in Subsection 9.1.3. The reactor pressure instruments of Nuclear Boiler System are discussed in Subsection 7.7.1.

The only other HP/LP interface exists in the Gravity Driven Cooling System (GDCS). Because the low pressure portion of GDCS has a design pressure equivalent to the reactor operating pressure, and its other end is open to the GDCS pools, there is no need for overpressure protection of the low pressure portion. An interlock is provided to prevent inadvertent manual initiation of the system during normal reactor operation. The GDCS design is discussed in Subsection 7.3.1.2.

7.6.1.2 System Description

Function Identification - Normally closed isolation valves consisting of an air-operated check valve and a motor-operated gate valve are provided to protect the FAPCS low pressure piping from over-pressurization during reactor power operation. The HP/LP interlock is provided to prevent the isolation valve from opening, and to close the isolation valve, if open, whenever a high reactor pressure signal from the Nuclear Boiler System (NBS) is present.

Power Sources - The power supplies for the reactor pressure instrument and valve control circuit are provided from reliable Class 1E power supplies, which are automatically connected to on-site power sources, in the event of loss of off-site power.

Equipment Design —Redundant reactor pressure instruments provide a high pressure signal to the FAPCS HP/LP interlock when the reactor pressure exceeds the setpoint determined, based on the design pressure of the low pressure FAPCS piping. Upon receipt of a high reactor pressure signal, the HP/LP interlock sends a signal to close the isolation valves and prevent them from opening.

Circuit Description - The HP/LP interlock circuit is designed to process the redundant high reactor pressure signals from NBS to determine whether a high pressure condition exists in the RWCU/SDC discharge line. If the high pressure condition exists, the interlock circuit sends a valve close signal to the LPCI line isolation valve control circuit.

Logic Sequencing - Upon receipt of the high reactor pressure signals from the redundant reactor pressure instruments, the following sequence occurs:

- HP/LP interlock circuit processes the signals and determines whether a high pressure condition exists in the RWCU/SDC discharge line.
- If the circuit determines that the high pressure condition exists, it sends a valve close signal to the LPCI line isolation valve control circuit.
- The valve control circuit closes the LPCI line isolation valve, if open, and prevents it from opening.

Bypasses and Interlocks - The HP/LP interlock design has no bypass or interlock features.

Redundancy and Diversity - The LPCI line uses redundant isolation valves in series for the overpressure protection when the reactor pressure is above the FAPCS design pressure. Diversity is provided by having a check valve equipped with pneumatic-assist actuator that has a fail close feature, and an electric power-assisted motor operated valve.

Actuated Devices - The LPCI line motor-operated isolation valve is the actuation device that is affected by the high pressure/low pressure (HP/LP) interlock.

Separation - Redundant reactor pressure signals are from separate instruments discussed in Subsection 7.7.1.

Testability - Testing of the reactor pressure instrument is discussed in Subsection 7.7.1.

The LPCI line isolation valves are stroke tested only during low reactor pressure conditions due to the interlock. These valves are not subjected to Appendix J leak rate test, because they are neither containment isolation valves nor reactor coolant pressure boundary. However, they are leak rate tested per ASME Code Section XI.

Environmental Considerations - The instrumentation and control for the HP/LP interlock are classified as Class 1E equipment and thus qualified according to the environmental conditions of the locations of the devices.

Operational Consideration - The HP/LP interlock prevents manual initiation of the LPCI mode of FAPCS until the reactor vessel has been depressurized to a pressure below the reactor pressure instrument setpoint.

Reactor Operator Information - The status of each valve providing the HP/LP boundary is indicated in the main control room (MCR). The state of the sensors is also indicated in the MCR.

Setpoints - The setpoint is based on the highest design pressure of the low pressure FAPCS piping.

7.6.1.3 Safety Evaluation

The ESBWR does not have a HP/LP interface involving safety-related system. There is a nonsafety-related HP/LP interface involving the low pressure FAPCS LPCI line, which interfaces with the high pressure condition in the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system piping. The RWCU/SDC system piping interfaces with the feedwater line, which maintains the reactor coolant pressure boundary.

General Functional Requirements Conformance - The FAPCS high pressure/low pressure interlock prevents opening of the injection valve on the LPCI discharge line. The interlock prohibits the LPCI line isolation valve from being opened whenever the reactor pressure is greater than the reactor pressure permissive setpoint for the interlock, thereby protecting the low pressure FAPCS piping from over-pressurization during reactor power operation. The interlock is designed to permit LPCI mode initiation when the reactor pressure is below the reactor pressure permissive setpoint allowing the operator to manually open the isolation valve. The interlock operates automatically, and its status is provided to the reactor operator in the MCR.

Specific Regulatory Requirements Conformance - Table 7.1-1 identifies applicable regulatory criteria, and industry codes and standards applied to the interlock system in accordance with the Standard Review Plan (SRP). These are addressed as follows:

10 CFR 50.55 and 52

- 50.55a(a)(1), Quality Standards for Systems Important to Safety

  Conformance: The HP/LP interlocks comply with this requirement.

- 50.55a(h), Criteria for Protection Systems for Nuclear Power Generating Stations (ANSI/IEEE Standard 279)

  Conformance: Separation and isolation is preserved both mechanically and electrically in accordance with IEEE 603 (this replaces IEEE 279) and RG 1.75. Electrical separation is maintained between the redundant divisions.

- 50.34(f)(2)(v)(I.D.3), Bypass and Inoperable Status Indication

  Conformance: The HP/LP interlock does not have a bypass feature.

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.47(a)(2), Level of Detail

- Conformance: The level of detail provided for the interlock systems within the Tier 1 and Tier 2 documents conform with this criterion.

- 52.47(b)(2)(i), Innovative Means of Accomplishing Safety Functions

  Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.6, and with Table 7.1-1, the following GDC are addressed:

- Criteria: GDC 1, 2, 4, 13, 19, 24 and 25.

  Conformance: The HP/LP interlocks do not involve reactivity control, hence GDC 25 is not applicable. The interlocks are in compliance with the remaining GDC listed above. The GDC are generically addressed in Subsection 3.1.2.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.6, and with Table 7.1-1, the following Regulatory Guides (RGs) are addressed for the H/LP interlocks:

- RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems
- RG 1.53 - Application of the Single Failure Criterion to Nuclear Power Protection Systems
- RG 1.75 - Physical Independence of Electrical Systems
- RG 1.105 – Setpoints for Safety-Related Instrumentation
- RG 1.118 - Periodic Testing of Electric Power and Protection Systems
- RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems

Conformance: The HP/LP interlocks conform to all of the above listed RGs with the assumption that the same interpretations and clarifications identified in Subsection 7.1.2.2 also apply.

RGs 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are addressed in conjunction with the Safety System Logic and Control (SSLC) system in Subsections 7.3.4 and 7.1.2.2.

Branch Technical Positions (BTPs)

In accordance with the Standard Review Plan for Section 7.6, and with Table 7.1-1, the following BTPs are addressed for the HP/LP interlocks:

- HICB-1 – Guidance on Isolation of Low-Pressure Systems from the High-Pressure Reactor Coolant System
- HICB-11 – Guidance on Application and Qualification of Isolation Devices
- HICB-12 – Guidance on Establishing and Maintaining Instrument Setpoints

- HICB-14 - Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems
- HICB-16 – Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52
- HICB-17 – Guidance on Self-Test and Surveillance Test Provisions
- HICB-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems
- HICB-21 – Guidance on Digital Computer Real-Time Performance

Conformance: The Interlock System complies with all the above BTPs. Discussion of BTPs HICB 14, 17, 18 and 21 are addressed in conjunction with the Safety System Logic and Control System (SSLC) in Subsections 7.3.4 and 7.1.2.2.

TMI Action Plan Requirements: In accordance with the SRP for 7.6 and with Table 7.1-1, 10 CFR 50.34(f)(2)(v) (I.D.3) applies to the HP/LP interlocks. This is addressed above. TMI action plan requirements are generically addressed in Appendix 1A.

7.6.2 Other Interlocks

The ESBWR design has no interlocks that isolate safety-related from nonsafety-related piping during LOCA.

7.6.3 COL Information

None.

7.6.4 References

None.

7.7 CONTROL SYSTEMS

This section describes the instrumentation and control systems for normal plant operation that are not essential to perform the safety functions of the plant, but those that control plant processes having a significant impact on plant safety. These systems can affect the performance of critical safety functions either through normal operation or through inadvertent operation. The control systems described in this section include:

- The Nuclear Boiler System
- Rod Control and Information System
- Feedwater Control System
- Plant Automation System
- Steam Bypass and Pressure Control System
- Neutron Monitoring System – Nonsafety-Related Subsystems
- Containment Inerting System

7.7.1 Nuclear Boiler System

The Nuclear Boiler System (NBS) instrumentation provides monitoring and control input for operational variables during normal plant operating modes and during plant response to accidents. The NBS sensors used for safety-related system actuation and control functions are addressed in the safety-related sections within this chapter. The safety-related NBS instrumentation only used for indication and instruments used for actuation and control of nonsafety-related systems are described in this subsection.

7.7.1.1 Design Bases

Safety (10 CFR 50.2) Design Basis

The NBS controls and instrumentation shall meet the following safety-related requirements:

- Provide reactor water level and dome pressure measurements over ranges and to accuracies necessary for adequate operator monitoring of reactor water level during normal, transient, and accident conditions.
- Provide qualification of reactor water level and dome pressure instrumentation for the design basis loadings of the safe shutdown earthquake (SSE), loadings associated with design basis accidents, and the environmental conditions associated with design basis accidents.
- Provide redundancy such that a single failure would not result in the loss of level and pressure indication.

Power Generation (Non-safety) Design Bases

The NBS instrumentation shall meet the following power generation requirements:

- Provide indication for the following parameters in support of normal plant operations;

- Reactor coolant and vessel temperatures;
- Reactor vessel water level,
  - Shutdown range,
  - Narrow range;
- Reactor vessel pressure;
- Safety/relief valve discharge line temperature; and
- To the extent practical, provide for periodic calibration and testing of the instrumentation during plant operation.

7.7.1.2 System Description

Summary Description

The NBS instruments and systems are used to provide the operator with information during normal plant operation and during transient and accident responses. The instrumentation discussed in this subsection is also discussed in Section 5.1, and shown on NBS ADS Initiation Logic, Figure 7.3-1.

Safety-related instrumentation is classified as Class 1E and is powered from Class 1E 250 VDC plant battery buses and 120 VAC uninterruptible power supplies. Nonsafety-related instruments are powered from the non-Class 1E instrument buses.

For instruments that are located below the process tap, including the RPV water level measurements, the sensing line slopes downward from the process tap to the instrument to preclude air traps.

Where it is impractical to locate the instruments below the process connection, the sensing lines descend below the process connection before sloping upward to a high point vent located at an accessible location with a fill connection. This permits filling and venting of noncondensable gases from the sensing line during calibration procedures.

Level and pressure sensing lines are connected to the reactor coolant pressure boundary (RCPB) and are classified as Quality Group A, ASME Section III, Class 1, and Seismic Category 1 up to the outboard excess flow check valve. The typical arrangement for these sensing lines includes a restricting orifice located inside containment, and a manual isolation valve located outside containment followed by an excess flow check valve.

Detailed System Description

Reactor Coolant and Vessel Temperature Monitoring - The reactor coolant temperatures are measured at the mid-vessel inlet to the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system and at the bottom head drain. Coolant temperature can also be determined in the steam filled parts of the RPV and steam-water mixture by measuring reactor pressure (which in the saturated system infers saturation temperature). Coolant temperatures (core inlet temperature) can normally be measured by the redundant core inlet temperature sensors located in each LPRM assembly below core plate elevation.

Reactor pressure vessel (RPV) outside surface temperature is measured at the head flange and bottom head locations.

Temperatures needed for operation and for compliance with the technical specification operating limits are obtained from these measurements.

Reactor Vessel Water Level

Figure 7.7-1 shows the water level range and the vessel penetrations for each water level range. The instruments are differential pressure devices calibrated for the specific vessel conditions (pressure and liquid temperature) conditions. The reactor water level instrumentation is referenced to a common reference zero: the top of active fuel (TAF).

Reactor water level instrumentation that initiates safety-related systems and engineered safeguards systems is discussed in Subsections 7.2.1 and 7.3.1. Reactor water level instrumentation that is used as part of the Feedwater Control System (FWCS) is discussed in Subsection 7.7.3.

Shutdown Range Water Level - This range is used to monitor the reactor water level during shutdown conditions when the head is removed and the reactor system may be flooded for refueling or maintenance. The water level measurement design method is the condensing chamber reference leg type. The vessel temperature and pressure conditions that are used for the calibration are given in Section 5.1. The two vessel instrument nozzle elevations used for this water level measurement are located at the top of the RPV head and just below the bottom of the dryer skirt.

Narrow Range Water Level - This range uses the RPV taps near the top of the steam outlet nozzle and the taps near the bottom of the dryer skirt. The instruments are calibrated to be accurate during the normal reactor operating conditions. The method of water level measurement is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The FWCS uses this range for its water level control and indication inputs. Refer to Subsection 7.7.3 for more information on the FWCS.

Wide Range Water Level - This range uses the RPV taps above the top of the active fuel. The upper taps are the same as the Narrow Range Water Level. The instruments are calibrated to be accurate at normal power operating conditions. The water level measurement method is the condensing chamber reference leg type and uses differential pressure devices as its primary elements. The RPV wide range water level instrumentation is both safety-related and nonsafety related (for DPS) and is provided for the range of normal, transient, and accident conditions. Separate sensors and indicators are provided for wide range level indication.

Fuel Zone Range Water Level - This range uses the RPV taps near the top of the steam outlet nozzle and the taps below the bottom of the active fuel. The instruments are calibrated to be accurate at 0 Pa gauge (0 psig) and saturated conditions. The water level measurement method is the condensing chamber reference type and uses differential pressure devices as its primary elements. The RPV fuel zone water level instrumentation is safety related and is provided for post-accident monitoring situations in which the water level may be substantially below the normal range. Separate sensors and indicators are provided for wide range level indication.

Reactor Vessel Pressure - Pressure transmitters detect reactor vessel pressure from the same instrument lines used for measuring reactor vessel water level, and provide indication in the

control room. The following lists the subsections in which other reactor vessel pressure measuring functions are discussed.

- Pressure transmitters and trip actuators for initiating scram, and pressure transmitters and trip actuators for bypassing the main steam line isolation valve closure scram are discussed in Subsection 7.2.1.
- Pressure transmitters that are used for pressure recording are discussed in Subsection 7.5.1.

Safety/Relief Valve Leak Detection - Thermocouples are located in the discharge pipes of eight safety/relief valves. The temperature signals are recorded and temperatures indicative of leaking safety/relief valve are alarmed in the main control room.

7.7.1.3 Safety Evaluation

The safety-related reactor water level and dome pressure instruments are designed to withstand the loads and environmental conditions under which they must function. Sufficient separate sensors and indicators are provided so that a single failure cannot result in the loss of level indication. The combined range of the wide range and fuel zone instrumentation ensures that adequate level information is available over the full extent of postulated design basis accident conditions.

The nonsafety-related instruments discussed in this subsection are designed to operate under normal and peak operating conditions of system pressures and ambient pressures and temperatures. Any mechanical interface of nonsafety-related instruments with safety-related instrument piping or the reactor coolant pressure boundary (RCPB) is classified as safety-related to avoid compromise of the Class 1E sensing capability and/or the RCPB. Should a line break occur in a nonsafety-related portion of a sensing line, the excess flow check valve would close to stop the flow of reactor coolant. In the event of a single failure of the excess flow check valve, the restriction orifice limits the flow of coolant to within acceptable bounds.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies Control Systems (including the NBS instrumentation) and the applicable codes and standards. These are discussed below. Codes and standards applicable to the safety-related monitoring functions of the wide range and fuel zone water level indication are discussed in Section 7.5.

10 CFR 50.55a(1) and 10 CFR 50.55a(h)

The NBS complies with these criteria.

10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Resolution of unresolved and generic safety issues is discussed in Section 1.11

10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications

ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii) Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.47(a)(2) Level of Detail

The level of detail provided for the NBS within the Tier 1 and Tier 2 documents conforms to this BTP.

10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria

In accordance with the SRP for Subsection 7.7 and Table 7.1-1, the following GDC are addressed for the NBS:

- Criteria: GDC 1, 2, 4, 13, 19 and 24
- Conformance: The NBS complies with these GDC.

SRM to SECY 93-087 II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems)

Conformance: In addition to the design features already incorporated in the design on defense-in-depth and against common mode failures as addressed to this SRM, the NBS (ADS) function and other Engineered Safety Features (ESF) designs conform with the Item II.Q of SECY-93-087 (BTP HICB-19) by the implementation of an additional Diverse Instrumentation and Control System, described in Section 7.8

Regulatory Guides

Regulatory Guide 1.75 - The NBS complies with RG 1.75.

Regulatory Guide 1.105 - The NBS complies with RG 1.105 as delineated in Subsection 7.1.2.2.

Regulatory Guides 1.151 - RG 1.151 - Instrument Sensing Lines

The instrument sensing lines for the NBS instrumentation are in full conformance with the guidelines of RG 1.151 and ISA-S67.02. Flow restrictors are provided inside containment on instrument lines connected to the reactor coolant pressure boundary. Accessible manual isolation valves and self-actuating excess flow check valves are provided outside the drywell. The mechanical design guidelines as defined by ISAS67.02 and RG 1.151 are met as applicable for each installation.

Regulatory Guide 1.153 - Consistent with the discussion of other regulatory guides and the General Design Criteria, the NBS complies with this regulatory guide.

Regulatory Guides 1.152, 1.168, 1.169, 1.170, 1.171, 1.172 and 1.173 are discussed in Subsection 7.1.2.2.

Branch Technical Positions (BTPs)

HICB-11 - The approach to compliance with RG 1.75 and RG 1.153 is discussed above.

HICB-12 - The Standby Liquid Control (SLC) system complies with BTP HICB-12.

HICB-16 - The level of detail provided for NBS in Tier 1 and Tier 2 documentation complies with BTP HICB-16.

BTP's HICB-14, HICB-17, HICB-18, HICB-19 and HICB-21 are discussed in association with the SSLC in Subsection 7.3.4.3, and in Subsection 7.1.2.2.

7.7.1.4 Testing and Inspection Requirements

Calibration and testing of the various instruments are performed during preoperational testing to confirm the instrumentation is installed correctly and perform as required.

Pressure, differential pressure, water level, and flow instruments are located outside the drywell so that calibration and test signals can be applied during reactor operation. Temperature elements located inside the drywell can be tested and calibrated from junction boxes located outside the drywell.

7.7.1.5 Instrumentation Requirements

The following information is available to the reactor operator from the instrumentation discussed in this subsection:

- Reactor water level is indicated in the main control room on displays associated with the different water level ranges.
- The reactor pressure is indicated in the main control room and at four local racks in the containment.
- The discharge line temperatures of the safety/relief valves (SRVs) are viewed on the VDUs in the main control room. Any temperature exceeding the trip setting is alarmed, indicating leakage of a safety/relief valve seat.
- RPV temperature is indicated and recorded in the main control room and low temperature is alarmed in the main control room.

7.7.2 Rod Control and Information System

7.7.2.1 Design Bases

Safety (10 CFR 50.2) Design Basis

The Rod Control and Information System (RC&IS) has no functional safety-related design bases and is designed such that functional capabilities of safety-related systems are not adversely affected.

Power Generation (Non-safety) Design Bases

The main objective of the RC&IS is to provide the capability to control the fine motion control rod drive (FMCRD) motors of the Control Rod Drive System (CRD) (explained in Subsections 4.6.1 and 4.6.2) to permit changes in core reactivity so that reactor power level and power distribution can be controlled.

RC&IS, by controlling the FMCRD motors and brakes of the CRD, by acquiring status and control rod position information from the FMCRD instrumentation of CRD and by sending purge water valve control signals to and acquiring status signals from the hydraulic control units (HCUs) of CRD, and by sending and receiving status and control signals to and from other plant systems and the various RC&IS modules, performs the following functions:

- Controls changes to the core reactivity, and thereby reactor power, by moving neutron absorbing control rods within the reactor core as initiated by:
  - The plant operator, when the RC&IS is placed in manual or semiautomatic mode of operation
  - The automatic rod movement mode of the Plant Automation System (PAS), when RC&IS is placed in automatic mode of operation.
- Displays summary information to the plant operator about positions of the control rods in the core and status of the FMCRDs and RC&IS. This summary information is provided by a RC&IS dedicated operator interface (DOI) on the main control panel. There are dual-redundant measurements of the absolute rod position during normal FMCRD conditions. If one position detector fails for an individual FMCRD, the failed position detector can be bypassed and the unit can continue to operate without power restrictions.
- Provides RC&IS and FMCRD status data and control rod position data to other plant systems that require such data (e.g., the Non-Essential DCIS).
- Provides for automatic, electric-motor run-in of all operable control rods following detection of activation of the hydraulic insertion of the control rods by a reactor scram. This function is called the scram-follow function.
- Automatically enforces rod movement blocks to prevent potentially undesirable rod movements (these blocks do not impact a hydraulic scram insertion function, the scram-follow function, the alternate rod insertion (ARI) function, or the selected control rod run-in (SCRRI) function).
- Provides for both manual and automatic insertion of all control rods, by an alternate and diverse method. This function is called the ARI motor run-in function. The associated ARI activation signals (i.e. activated if either the automatic or manual ARI function is activated by NE-DCIS scope logic) are provided to RC&IS from the Non-Essential Distributed Control and Information System (NE-DCIS). RC&IS logic has been designed such that a single failure, only in the single-channel FMCRD control logic and equipment associated with one FMCRD, may result in insertion failure of that rod when the ARI function is activated.
- Provides for insertion of selected control rods: 1) for mitigation of a loss of feedwater heating event; or 2) for providing needed power reduction after occurrence of a load rejection event or a turbine trip event (that does not result in scram). This function is called the SCRRI function, which is automatically activated based upon receiving SCRRI command signals from the NE-DCIS (manual initiation capability based upon simultaneous actuation of two manual SCRRI pushbuttons located on the main control console in the main control room also exists).

- Insures that the pattern of control rods in the reactor is consistent with specific control rod pattern restrictions. This function is performed by the Rod Worth Minimizer (RWM) subsystem of the RC&IS and is effective only when reactor power is below the low power setpoint (LPSP).
- Enforces fuel operating thermal limits minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) when reactor power is above the low power setpoint (LPSP). This function is performed by the automated thermal limit monitor subsystem (ATLM) of the RC&IS.
- Provides the capability for conducting FMCRD-related surveillance tests, including periodic individual HCU scram performance testing.
- Through the capabilities of the gang rod selection and verification logic of the rod action and position information (RAPI) subsystem, enforces adherence to a predetermined rod pull/insert sequence, called the reference rod pull sequence (RRPS) during both automatic and semi-automatic rod movements.

7.7.2.2 System Description

A simplified, typical RC&IS block diagram is shown in Figure 7.7-2. This drawing depicts the major components of the RC&IS, their interconnections and interfaces with other plant systems.

7.7.2.2.1 System Configuration

RC&IS utilizes a dual-redundant architecture of two independent channels for normal monitoring of control rod positions and executing normal control rod movement commands. Under normal conditions, each channel receives separate input signals and both channels perform the same functions. The outputs of the two channels are continuously compared. For normal functions of enforcing and monitoring control rod positions and emergency rod insertion, the outputs of the two channels must be in agreement. Any sustained disagreement between the two channels would result in a rod block. However, when the conditions for generating a rod block signal in a single channel are satisfied, that channel alone (and independent of the other) can issue a rod block signal. For the FMCRD emergency insertion functions (Scram- Follow, ARI, SCRRI), 3-out-of-3 logic is used in the induction motor controller logic with the additional input signal coming from the associated emergency rod insertion panels. An automatic single channel bypass feature (only activated when an emergency insertion function is activated) is also provided to assure high availability for the emergency insertion functions when a single channel failure condition exists.

Failure or malfunction of RC&IS has no impact on the hydraulic scram function of CRD. The circuitry for normal insertion and withdrawal of control rods in RC&IS is completely independent of the Reactor Protection System (RPS) circuitry controlling the scram valves. This separation of the RPS scram and RC&IS normal rod control functions prevents failure in the RC&IS circuitry from affecting the scram circuitry.

The RC&IS consists of several different types of cabinets (or panels), which contain special electronic/electrical equipment modules for performing RC&IS logic in the reactor building (RB) and control building (CB) and a DOI on the main control panel in the MCR. The RC&IS DOI provides summary information to the plant operator with respect to control rod positions,

FMCRD and RC&IS status and HCU status. Controls are also provided for performing normal rod movement functions, bypassing of major RC&IS subsystems, performing CRD surveillance tests (except the FMCRD holding brake testing performed during a refueling outage), and resetting RC&IS trips and most abnormal status conditions (a few abnormal status conditions require reset actions at local control panel equipment). There are nine types of electronic/electrical cabinets/panels that perform logic functions of the RC&IS:

(1) Rods Action Control Subsystem (RACS) Cabinets

There are two types of cabinets in the back-panel area referred to as the RACS, consisting of rod action and position information (RAPI) panels and an ATLM/RWM panel, which provide for a dual-redundant architecture. The RAPI panels consist of a RAPI-A panel and RAPI-B panel with the channel A logic in the RAPI-A panel and the channel B logic in the RAPI-B panel. In addition, the RAPI-A panel includes the RAPI DOI, which displays the same information that is available on the RC&IS DOI in the MCR. The RAPI DOI also serves as a backup for the RC&IS DOI control capabilities, should the RC&IS DOI become unavailable. A hard switch located in the RAPI-A panel is used to change the selection of DOI control operation capability between the RC&IS DOI and the RAPI DOI (i.e. only one of these DOIs can be selected for control capability at any given time). Normally the RC&IS DOI is selected for control functions instead of the RAPI DOI. The following sections will describe the normal situation of the RC&IS DOI being selected for control capability.

The ATLM/RWM panel contains two channels of logic for the automated thermal limit monitor (ATLM), the rod worth minimizer (RWM) and the RAPI signal interface units (SIUs).

(2) Remote Communication Cabinets (RCCs)

The RCCs are located in sets that each contains a dual channel file control module (FCM). The FCMs interface with the rod server modules (RSMs) that are contained in the same set of cabinets, and interface with the RAPI subsystems in the MCR, via the RC&IS multiplexing network. Each RSM is composed of logic for two Rod Server Processing Channels (RSPCs A and B) so that there is a dual-redundant logic design for each RSM and associated Resolver-to-Digital Converters (RDCs A and B) that provide for conversion of the Resolver A and Resolver B analog signals of the CRD system into two independent digital representations of the absolute position of the corresponding FMCRD. The logic for both RSPCs receives the digital representations from both RDCs for use in the RSPC control and monitoring logic. The logic for each channel of RSPC may be implemented in the associated FCM channel equipment or may be located in a separate, replaceable RSPC module located in the RCC. Figure 7.7-2 shows an example representation with the logic of each RSPC channel implemented in a separate RSPC module. However, regardless of the final detailed RCC hardware configuration for RSPC logic implementation, channel A RSPC logic is implemented in separate equipment from the equipment in which the channel B RSPC logic is implemented, to maintain tolerance for single channel failures.

(3) Motor Controller Cabinets (MCCs)

The MCCs consist of motor control equipment required for turning on and off the AC power required for energization of the FMCRD 3-Phase motor and its directly associated

motor built-in brake for performing FMCRD movements. The control capability includes AC phase direction change for the 3-phase AC power supplied to each motor so that both insertion and withdrawal movements of each FMCRD can be accomplished. The motor built-in brake (MBB) provides for more accurate positioning control of each FMCRD because the de-engergization of this brake promptly after AC power is turned off by the motor control prevents excessive movement after the desired stopping position has been reached. Each motor controller includes logic to process rod movement commands received from the logic of the associated RSPCs in a RCC. Each motor control also provides status signals to the associated RSPCs. All motor controls also receive a separate discrete input signal from an Emergency Rod Insertion Panel that is used in the logic for providing the emergency rod insertion movement functions (i.e. scram-follow, ARI or SCRRI)..

(4) Rod Brake Controller Cabinets (RBCCs)

The RBCCs contain electrical and/or electronic logic and other associated electrical equipment for the proper operation of the FMCRD holding brakes. The Rod Brake Controllers (RBCs) receive signals for brake disengagement or engagement from the logic of the associated RSPCs. RBC logic provides two separate (channel A and channel B) brake status signals to the logic of the associated RSPCs.

(5) Emergency Rod Insertion Control Panel (ERICP)

The emergency rod insertion control panel is located in the back-panel area of the MCR. It serves as an additional logic panel to contain relays (or solid-state equivalent) hardware needed to transmit discrete output signals to the emergency rod insertion panels in the Reactor Building (RB). The discrete output signals are activated based upon input signals received from the RPS portion of the SSLC panels that indicate a scram-follow function is active or based upon input signals received from the Non-Essential Distributed Control and Information System (NE-DCIS) that indicate a ARI function or automatic SCRRI function is active or by input signals from the two manual SCRRI pushbuttons on the Main Control Room Panel (MCRP).

(6) Emergency Rod Insertion Panels (ERIPs)

The emergency rod insertion panels are located in the reactor building and provide discrete output signals to the IMCs in the MCCs. The discrete output signals are activated based upon input signals received from the emergency rod insertion control panel that indicate the scram-follow function, the ARI function or the SCRRI function is active.

(7) Scram Time Recording Panels (STRPs)

The scram time recording panels (STRPs), located in the RB, monitor the FMCRD position reed switch status using reed switch sensor modules (RSSMs) and communicate this information to the RAPI via the RC&IS multiplexing network. Also, the STRPs automatically record and time tag FMCRD scram timing position reed switch status changes either: 1) after initiation of an individual HCU scram test at the RPS Scram Time Test Panel, or 2) after a full-core reactor scram has been initiated. The recorded scram timing data can be transmitted to the scram time recording and analysis panel in the MCR back-panel area.

(8) Scram Time Recording and Analysis Panel (STRAP)

The STRAP, located in the MCR back-panel area, receives scram timing position information from the STRPs and performs scram timing performance analysis against the applicable Technical Specification requirements. The recorded performance information can also be transmitted to the Non-Essential DCIS equipment for further data analysis and archiving.

(9) Rod Action and Position Information (RAPI) Auxiliary Panels

(10) RAPI Auxiliary Panels, located in the Reactor Building, provide output signals to open a purge water valve whenever either FMCRD associated with the corresponding HCU receives an insertion command from RAPI subsystem. These panels also monitor scram valve position status as well as HCU accumulator water pressure and level status (i.e., normal or abnormal). Communication of this information to and from the RAPI subsystem is achieved via the NE-DCIS equipment. Two of the non-safety remote multiplexing unit cabinets of the NE-DCIS equipment scope are used as the RAPI auxiliary panels (i.e. the RAPI Auxiliary Panels are physically not part of RC&IS equipment scope, even though they provide for the RC&IS related functions described above).

7.7.2.2.2 RC&IS Multiplexing Network

RC&IS multiplexing network consists of two separate channels. Fiber-optic communication links are used in this multiplexing network to handle communication between the RACS and the RSPCs in the RCCs (via the FCMs), communication between the STRPs and the RACS, and communication between the STRPs and the STRAP. Communication between the RAPI auxiliary panels (for HCU purge water valve control and HCU status monitoring) and the RAPI channels is achieved by the non-essential DCIS equipment, not the RC&IS multiplexing network.

The plant essential E-DCIS communication equipment interfaces with FMCRD dual redundant separation switches (A and B) and provides the appropriate status signals to the RACS Cabinets to be used in the RC&IS logic for initiating rod block signals of the appropriate FMCRD if a separation occurs. The E-DCIS communication equipment provides these signals to the RAPI SIUs of the RC&IS via communication with the non-essential DCIS through proper isolation. The E-DCIS and NE-DCIS communication equipment are not part of the RC&IS equipment scope. Each RAPI SIU transmits these status signals to the associated RAPI channel for use in the RAPI rod block logic.

7.7.2.2.3 Classification

The RC&IS is not classified as a safety-related system, as it has a control design basis only and is not required for the safe and orderly shutdown of the plant. A failure of the RC&IS will not result in gross fuel damage. The rod block function of the RC&IS, however, is important in limiting the potential consequences of a rod withdrawal error during normal plant operation. An abnormal operating transient that might result in local fuel damage is prevented by the rod block functions of the RC&IS.

7.7.2.2.4 Power Sources

(1) Normal

The Low Voltage Distribution System provides the required incoming three-phase AC power for the induction motor controller equipment in order to provide a 3-phase AC power source required for energization of the associated FMCRD induction motors and motor built-in brakes by the IMCCs. The Low Voltage Distribution System also provides the required AC power for the rod brake controller power supplies in the RBCCs, the emergency rod insertion panels and the associated emergency rod insertion control panel. The Medium Voltage Distribution System power bus and equipment design assures that the associated Low Voltage Distribution System equipment that provides required AC power to the IMCCs, RBCCs and ERIPs will be automatically powered from the standby AC diesel generators should the normal power source be lost. Excitation power required for logic in the emergency rod insertion control panel is provided directly from the emergency rod insertion panels. The power distribution design provides three distinct electrical groups of power. The distribution of these three groups of electrical power to FMCRDs is such that approximately one third of the FMCRDs belong to each group. The distribution of FMCRDs in each electrical group is scattered throughout the reactor core such that complete insertion of the FMCRDs in any two of the three electrical groups to the full-in position will assure the reactor reaches hot shutdown conditions. This approach provides increased reliability for the capability of the motor run-in ARI function, if activated, to assure the reactor achieves hot shutdown conditions.

The power for all RC&IS equipment, except as noted above, is derived from two separate, non-divisional AC power sources (Chapter 8) with at least one of the redundant AC power sources being an uninterruptible AC power supply (UPS). Redundant power supplies are also provided for this equipment so that failure of a single power source or of a single power supply does not result in the complete loss of capability of the RC&IS to perform rod movements. For certain types power source or supply failures, the operator has to perform appropriate bypass of the affected RC&IS equipment in order to restore rod movement capability.

(2) Alternate

On loss of normal power source, the nonsafety-related standby diesel generators provide for an alternate power source for the IMCCs, RBCCs and emergency rod insertion panels.

7.7.2.2.5 RC&IS Scope

The RC&IS scope includes the following equipment:

(1) All the electrical/electronic equipment contained in the RACS cabinet, the RCCs, the IMCCs, the RBCCs, the STRPs, the STRAP, the emergency rod insertion panels, and the emergency rod insertion control panel. (NOTE: RAPI auxiliary panels are designated as part of non-essential DCIS).

(2) The RC&IS multiplexing network equipment.

(3) The cross-channel communication links between equipment located in the RACS cabinets.

(4) The dedicated RC&IS DOI and the communication links from the RACS cabinets to this interface.

7.7.2.2.6 RACS Cabinets Subsystems

As discussed previously, the rod action control subsystem cabinets each have four identical dual-channel subsystems; the RAPI, the RWM, the ATLM and the RAPI SIU. This section describes the key functions performed by each of these subsystems.

(1) The RAPI is the primary RC&IS equipment that performs the following functions:

a. Accepts and responds appropriately to manual, semi-automatic, and automatic rod movement commands.

b. Enforces rod blocks based upon signals both internal and external to RC&IS. Internal RC&IS signals include those initiated from either of the two channels of rod blocks initiated by signals from the ATLM, RWM, RAPI SIU equipment, and those caused by any RAPI two-channel disagreement. External input signals to each RAPI channel that are used for the rod block logic originate from:

The safety-related four divisions of the RPS (required isolation provided by RPS related equipment)

The safety-related four divisional Source Range Neutron Monitor (SRNM) and Average Power Range Monitor (APRM) subsystems of the Neutron Monitoring System (NMS) (required isolation provided by the NMS).

The safety-related FMCRD dual redundant separation switches (A & B) of each control rod via divisions I and II of E-DCIS communication (required isolation provided by non-essential DCIS equipment).

The non-safety dual-channel multi-channel rod block monitor (MRBM) of the NMS.

Refueling Equipment

c. Enforces adherence to a predetermined rod pull sequence that is stored in RRPS memory. The RRPS memory defines the order in which gangs of control rods are selected and moved when either semi-automatic or automatic rod movements are performed (i.e. the equivalent to the pull sheet used by plant operators when performing manual rod movements for conventional BWR plants). Violation of the RRPS causes RAPI logic to issue:

A switch to manual mode when RC&IS is in the Automatic rod movement mode or the Semi-automatic rod movement mode.

An alarm signal when RC&IS is in the Manual rod movement mode.

d. Provides control rod position and FMCRD status information to the NE-DCIS; to the NMS; to the RWM; and to the ATLM. The RAPI transmits signals required by the NMS, ATLM and RWM to the associated RAPI SIU which then transmits required status signals to both channels of the ATLM, RWM and the multi-rod block monitor (MRBM) channels of the NMS.

e. Provides the scram-follow function that automatically activates motor run-in of the ball nuts of all operable FMCRDs to the normal full-in position after a reactor scram has occurred. If the rapid hydraulic insertion function for any FMCRD does not work properly, this function provides an electrical motor driven backup means to achieve full insertion of all operable FMCRDs.

f. Provides the SCRRI function that results in automatic insertion of predefined control rods to specified target insertion positions so that required reactor power reduction is achieved when this function is activated.

g. Provides for alternate rod insertion motor run-in of all control rods (i.e., ARI), based on the receipt of the ARI initiation signals from the NE-DCIS

h. Sends rod movement commands to and receives rod position, FMCRD and RC&IS related status information from the logic of all of the rod server processing channels (A & B) of each RSM in the RCCs, by means of FCMs and the RC&IS multiplexing network. Also, receives FMCRD position reed switch status information from the STRPs, by means of the RC&IS multiplexing network.

i. Sends and receives information and control signals to and from the other RAPI channel.

j. Sends HCU purge water valve control signals to and receives HCU status signals from the NE-DCIS equipment.

k. Provides for performance of different CRD surveillance tests, including:

(i) Scram Time Test;

(ii) Coupling Check Test; and

(iii) Double-Notch Test

(2) The RWM issues a rod withdrawal block signal and a rod insertion block signal that is used in the RAPI rod block logic. This rod block signal ensures that:

a. Absolute rod pattern restrictions called the ganged withdrawal sequence restrictions (GWSR), when reactor power is below the low power setpoint (LPSP), are not violated (only applicable when the RPS reactor mode switch is in either STARTUP or RUN mode). The GWSR assure that control rod worths are maintained to within reasonable values by only allowing rod patterns that result in relatively low rod worths when control rods are withdrawn..

b. Only the two control rods associated with the same HCU can be withdrawn for the 2-CRD scram time test when the RPS reactor mode switch is in the REFUEL mode and the scram test mode has been activated. This function provides for performing individual HCU scram testing during planned refueling outages.

c. The RWM also includes logic for performing shutdown margin testing when the RPS reactor mode switch is in STARTUP mode. This mode allows only a limited set of pre-specified control rods to be withdrawn to perform this special testing.

d. The RAPI are responsible for enforcing the applicable RWM rod block by sending appropriate rod block signals to the logic of the RSPCs in the RCCs. Either channel of RWM can cause a rod block independently.

(3) The ATLM issues an internal rod withdrawal block signal within RC&IS. These signals, when RC&IS is in the Automatic rod movement mode, cause RC&IS to transfer to the manual rod movement mode. The ATLM-based rod block prevents violation of normal operating limit restrictions on fuel thermal limit values, i.e., minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) operating limits, had operations stayed in the automatic mode. The ATLM algorithm is based upon input signals from the local power range monitors (LPRMs) and average power range monitors (APRMs) of the NMS and control rod positions and status data and other plant data from the RAPI signals transmitted from RAPI channels via the RAPI SIUs. The ATLM operating limit setpoints may be updated based upon calculated inputs from the core monitoring function of NE-DCIS. Updates of the ATLM setpoints can occur either automatically or manually by the operator using NE-DCIS touch screen display capabilities (to request a manual ATLM update). Either channel of the ATLM can cause transfer to Manual mode from Automatic mode and rod withdrawal block initiation independently.

7.7.2.2.7 Rod Control and Information System Operation Description

7.7.2.2.7.1 Single Rod Movements

Though this mode of rod movement is not normally used, the capability exists for the plant operator to perform manual rod movements of individual control rods. To perform this type of rod movement, the operator must establish the manual, single rod movement mode by controls provided at the RC&IS DOI, and select the individual rod to be moved. After confirming the correct rod has been selected, the operator then establishes the desired rod movement mode among step movement (i.e. movements of 36.5 mm nominal distance for each step movement activated except for the last withdrawal or for the first step movement from normal full-out position, which has a nominal step distance of 37.5 mm), notch movement (i.e. movement to the next rod position that is an integer multiple of 2 steps movement from being fully- inserted), or continuous mode (for which rod movement continues as long as the operator activates a movement command, then settles to the effective target position after the operator deactivates the movement command). Then, to accomplish the desired movement in the selected movement mode, the operator activates “insert” or “withdraw” movement command (by activating associated hard pushbutton switches located adjacent to the RC&IS DOI on the main control panel in the MCR) and the desired rod movement will occur (provided that no abnormal conditions, such as a rod block, are activated). Should any of the higher priority automatic rod movement actions be activated (e.g. SCRRI, scram-follow or ARI), these movements will override the operator desired normal movement and will be completed as required. This is true no matter what mode of normal rod movement is activated.

The RAPI of the RC&IS enforces rod blocks based upon signals internal or external to the system. These rod blocks can prevent desired rod movements or stop rod movements, if activated while normal rod movements are underway. This applies to both single rod movement and ganged rod movement modes.

The internal signals include those signals from ATLM and RWM. If there is any disagreement between the two-channel logic of the subsystems of the RC&IS, rod block signals are transmitted to the rod server module, unless one of the channels of logic has been manually bypassed.

Examples of external input signals which could cause rod withdrawal blocks include those from the SRNM; average power range monitor (APRM) subsystems and the multi-channel rod block monitor subsystems of the NMS or from FMCRD separation status signals received from the E-DCIS via data transmission to the RC&IS. If the status of either separation switch A or B indicates that FMCRD separation has occurred, a rod withdrawal block condition is activated for the corresponding FMCRD if the RPS reactor mode switch is in either STARTUP or RUN mode and that rod is currently selected for normal movement. A more complete list of rod block conditions is provided later in this section.

When normal rod movements are performed (with no abnormal conditions existing), the RAPI of the RC&IS transmits the appropriate rod movement command signals to a dual channel file control module (FCM) located in a RCC. These rod movement command signals are received at the dual channel FCM and routed to logic for the associated rod server processing channel (RSPC) A and RSPC B of the rod server modules (RSMs) of the selected rod and then are transmitted as channel A and channel B inputs for the corresponding induction motor controller. Channel A and channel B brake energization signals are transmitted to the associated rod brake controller (RBC). The induction motor controller then performs two-out-two voting on the command signals received from the logic of both RSPCs and then activates the proper power control signals to accomplish the FMCRD motor movement (i.e. provides the required 3-phase AC power output to the FMCRD motor and power to the associated motor built-in brake to perform the desired movement). The rod brake controller similarly performs two-out-two voting and energizes (i.e. mechanically releases) the FMCRD holding brake just prior to the start of FMCRD motor movement and then de-energizes (i.e., mechanically engages) the FMCRD holding brake just after the desired normal rod movement is completed.

The RDCs of the RSM also interface with instrumentation of the FMCRD (a subsystem of the CRD), collects absolute rod position for the corresponding FMCRD by converting the resolver A and resolver B analog signals into digital data representing the FMCRD rod position for use in the associated RSPCs' logic and transmission (via the RC&IS multiplexing system) to the RAPI logic and for the RAPI to transmit rod position data to other systems and subsystems and to the RC&IS DOI.

7.7.2.2.7.2 Ganged Rod Movements

There are three means of controlling ganged rod motion. The RC&IS provides for automatic mode, semi-automatic, and manual mode. When in the automatic mode of operation, commands for insertion or withdrawal are received from the PAS.

The RC&IS DOI provides controls for activating automatic, semi-automatic, or manual rod movement mode of operation. When the system is in the semi-automatic mode, all rod movements are controlled by the operator. However, the RC&IS, by using a database called RRPS and keeping track of the current control rods' positions, provides for automatic selection of the next gang, as required, to perform the sequence of rod movements in accordance with the RRPS definition. By this approach, the operator only needs to decide when to either insert or

withdraw control rods and does not have to decide which gang of control rods to select next to assure the RRPS sequence is followed.

When the RC&IS is in manual mode and ganged rod movement mode has also been chosen, if the operator selects a specific rod in a gang, the logic will automatically select all associated rods in that gang. The operator does not have to follow the RRPS sequence when performing manual rod movements; however, in order to re-establish either semi-automatic or automatic rod movement modes, the operator will have to establish an initial rod pattern that is consistent with the RRPS allowed rod patterns.

When the automatic mode is active, the RC&IS responds to signals for rod movement request from the PAS. In this mode, the PAS simply requests either desired control rod insertion or withdrawal movements. The RC&IS responds to this request by using the RRPS and the current rods' positions and automatically selects the appropriate gang and executes the next in sequence withdrawal/insert commands as required.

In order for the automatic rod movement feature of the RC&IS to be active, the soft switch on the RC&IS dedicated operator interface for automatic rod movement mode must be activated with none of the abnormal conditions that could prevent RC&IS automatic operation mode being active. The operator has the option of discontinuing the automatic operation by either placing the RC&IS mode switches to manual mode or to semi-automatic mode.

7.7.2.2.7.3 Establishment of RRPS

The RRPS is normally established before plant startup and stored in memory of the NE-DCIS equipment and the RC&IS. The NE-DCIS and RC&IS allow modifications to be made to the RRPS through operator actions. The NE-DCIS provides compliance verification of the proposed changes to the RRPS with the ganged withdrawal sequence requirements.

The RC&IS provides a capability for an operator to request a download of the RRPS from the NE-DCIS. The new RRPS data is loaded into the RAPI. Download of the new RRPS data can only be completed when the RC&IS is in manual rod movement mode and when a permissive switch located at the RAPI-A panel is activated.

The RC&IS provides feedback signals to the NE-DCIS for confirming successful completion of downloading the RRPS data.

Rod withdrawal block signals are generated whenever selected single or ganged rod movements differ from those allowed by the RRPS, when the RC&IS is in either the automatic or semi-automatic rod movement mode.

The RC&IS provides for activation of an alarm at the operators panel for an RRPS violation.

7.7.2.2.7.4 Rod Block Function

The rod block logic of the RC&IS, upon receipt of input signals from other systems and internal RC&IS subsystems, inhibits movement of control rods. In most cases, only a rod withdrawal block is activated. However, the RWM can also activate a rod insertion block for enforcement of the ganged withdrawal sequence restrictions (GWSR).

Rod block signals to the RC&IS from Class 1E systems are appropriately isolated. This provides required isolation between safety and non-safety systems while keeping electrical failures from propagating into the safety systems or into the RC&IS.

The presence of any rod block signal, in either channel or both channels of the RC&IS logic, causes the automatic changeover from automatic mode to manual mode. The automatic rod movement mode can be restored by taking the appropriate action to clear the rod block and by using the selector switch to restore the automatic rod movement mode.

If either channel or both channels of the RC&IS logic receive(s) a signal from any of the following type of conditions, a rod block is initiated:

(1) Rod separation detection (rod withdrawal block only for those selected rod(s) for which the separation condition is detected and are not in the INOPERABLE BYPASS condition, applicable when the RPS reactor mode switch is in STARTUP or RUN).

(2) Reactor mode switch in SHUTDOWN (rod withdrawal block for all control rods, applicable when the RPS reactor mode switch is in SHUTDOWN).

(3) Startup Range Neutron Monitor (SRNM) withdrawal block (rod withdrawal block for all control rods, not applicable when the RPS reactor mode switch is in RUN).

(4) Average Power Range Monitor (APRM) withdrawal block (rod withdrawal block for all control rods).

(5) CRD charging water low pressure (rod withdrawal block for all control rods).

(6) CRD charging water low-pressure trip bypass (rod withdrawal block for all control rods).

(7) RWM withdrawal block (rod withdrawal block for all control rods, applicable below the Low Power Setpoint).

(8) RWM insert block (rod insertion block for all control rods, applicable below the Low Power Setpoint).

(9) ATLM withdrawal block (rod withdrawal block for all control rods, not applicable below the Low Power Setpoint).

(10) Multi-channel Rod Block Monitor (MRBM) withdrawal block (rod withdrawal block for all control rods, not applicable below the Low Power Setpoint).

(11) Gang large deviation (i.e. gang misalignment) withdrawal block (rod withdrawal block for all operable control rods of the selected gang, applicable when RC&IS GANG mode selection is active).

(12) REFUEL mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS reactor mode switch is in REFUEL if a fuel bundle is being handled by the refueling platform while positioned over the reactor pressure vessel).

(13) STARTUP mode withdrawal block (rod withdrawal block for all control rods, applicable when the RPS reactor mode switch is in STARTUP if the refueling platform is positioned over the reactor pressure vessel).

(14) Rod Action and Position Information (RAPI) trouble (rod withdrawal block and rod insertion block for all control rods).

(15) RAPI Signal Interface Unit (SIU) trouble (rod withdrawal block for all control rods).

(16) Electrical group power abnormal (rod withdrawal block and rod insertion block for all control rods).

The RC&IS enforces all rod blocks until the rod block condition is cleared. The bypass capabilities of the RC&IS permit clearing certain rod block conditions that are caused by failures or problems that exist in only one channel of the logic.

7.7.2.2.7.5 RC&IS Reliability

The RC&IS has a high reliability and availability due to the dual channel configuration in its design that allows its continual operation, when practicable, in the presence of component hardware failures. This is achieved by the operator being able to reconfigure the operation of the RC&IS through bypass capabilities while the failures are being repaired.

The expected system availability during its 60-year life exceeds 0.99. The expected reliability is based upon the expected frequency of an inadvertent movement of more than one control rod. The expected frequency of an inadvertent movement of more than one control rod, due to failure, is less than or equal to once in 100 reactor operating years.

The RC&IS design assures that no credible single failure or single operator error can cause or require a scram or require a plant shutdown. The RC&IS design preferentially fails in a manner that results in no further normal rod movement.

7.7.2.2.7.6 RC&IS Bypass Capabilities

The RC&IS provides the capability to bypass resolver A (or resolver B), if it is bad, and select resolver B (or resolver A) for providing rod position data to both channels of the RC&IS. The RC&IS logic prevents the simultaneous bypassing of both resolver signals for an individual FMCRD.

The RC&IS allows the operator to completely bypass up to eight control rods by declaring them “Inoperable” and placing them in this bypass condition (except that more control rods can be bypassed when the RPS reactor mode switch is in REFUEL mode, as described below). Through operator action, an update in the status of the control rods placed into “inoperable” bypassed can be performed at the RC&IS DOI.

Activating a new RC&IS “Inoperable Bypass Status” to the RAPI is only allowed when the RC&IS is in a manual rod movement mode and when a bypass permissive switch located near the RC&IS DOI on the main control panel in the MCR is activated.

The operator can substitute a position for the rod that has been placed in this bypass state into both channels of the RC&IS, if the substitute position feature is used. The substituted rod position value entered by the operator is used as the effective measured rod position that is stored in both RAPI channels and sent to other subsystems of the RC&IS and to other plant systems (e.g., the NE-DCIS). The position substitution status of each FMCRD can also be displayed at the RC&IS DOI and the RAPI DOI.

For purposes of conducting periodical inspections on FMCRD components, RC&IS allows placing up to 54 control rods in “inoperable” bypass condition, only when the RPS reactor mode switch is in REFUEL mode.

The RC&IS enforces effective rod movement blocks when the control rod has been placed in an inoperative bypass status. This is accomplished by the RC&IS logic by not sending any rod movement and brake energization power to the associated FMCRD, when this bypass status is active.

In response to activation of either normal rod movement or special insertion functions, such as ARI, control rods in this bypass condition do not respond to movement commands.

The RC&IS single/dual rod sequence restriction override bypass feature allows the operator to perform special dual or single rod scram time surveillance testing at any power level of the reactor. In order to perform this test, it is often necessary to perform single or HCU pair rod movements that are not allowed normally by the sequence restrictions of the RC&IS.

When a control rod or pair of control rods associated with an individual HCU is placed in a S/DRSRO bypass condition, those control rod(s) are no longer used in determining compliance to the RC&IS sequence restrictions (e.g., the ganged withdrawal sequence and RRPS).

The operator can only perform manual rod movements of control rods in the S/DRSRO bypass condition. The logic of the RC&IS allows this manual single/dual rod withdrawal for special scram time surveillance testing.

The operator can place up to two control rods associated with the same HCU in the S/DRSRO bypass condition.

The dedicated RC&IS DOI display information contains status indication of control rods in a S/DRSRO bypass condition.

The RC&IS ensures that S/DRSRO bypass logic conditions have no effect on special insertion functions for an ARI, SCRRI, or SCRAM following condition and also no effect on other rod block functions, such as MRBM, APRM, or SRNM rod blocks.

The drive insertion following a single/dual rod scram test occurs automatically. The operator makes the necessary adjustment of control rods in the system prior to the start of test for insertions, and restores the control rod to the desired positions after test completion.

In addition to the RC&IS bypass functions that affect both channels (i.e. the bypass capabilities described previously), there are additional RC&IS bypass functions provided for the operator to establish bypass conditions that affect only one channel of the RC&IS. The interlock logic prevents the operator from placing both channels in bypass for these types of bypass conditions. Logic enforces bypass conditions to ensure that the capability to perform any special function (such as an ARI, scram following, and SCRRI) is not prevented by these bypass conditions.

The RC&IS logic ensures that associated special restrictions that are placed on the plant operation are enforced as specified in the applicable plant Technical Specifications for invoked bypass conditions that affect a single channel.

The status and extent of the bypass functions can be determined at the RC&IS DOI.

Bypass conditions generally allow continuation of normal rod movement capability by bypassing failed equipment in one RC&IS channel. After repair or replacement of the failed equipment is completed, the operator can restore the system or subsystem to a full two-channel operability. The operator has the capability to establish single-channel bypass conditions within the following system or subsystems.

- RSPC channel A or B bypass.
- FCM channel A or B bypass.
- ATLM channel A or B bypass.
- RWM channel A or B bypass.
- RAPI channel A or B bypass.

7.7.2.2.7.7 ATLM Algorithm Description

The ATLM is a microprocessor-based subsystem of the RC&IS that executes two different algorithms for enforcing fuel operating thermal limits when reactor power is above low power setpoint. One algorithm enforces operating limit minimum critical power ratio (OLMCPR), and the other the operating limit minimum linear heat generation rate (OLMLHGR). For the OLMCPR algorithm, the core is divided into multiple regions, each region consisting of 16 fuel bundles. For the OLMLHGR algorithm, each region is further vertically divided up into four segments. During a calculation cycle of ATLM rod block setpoints (RBS) are calculated for OLMCPR monitoring and for OLMLHGR monitoring. Then the calculated setpoints are compared with the real time averaged LPRM readings for each region/segment. The ATLM issues a trip signal if any regionally averaged LPRM reading exceeds the calculated RBS. This trip signal causes a rod block within the RC&IS.

The ATLM algorithm is also based upon control rod positions and status data and other plant data from the RAPI. The ATLM operating limit setpoints may be updated based upon calculated inputs from the core monitoring function of the NE-DCIS. Updates of the ATLM setpoints can occur either automatically or by operator request.

7.7.2.2.7.8 Operational Considerations

RC&IS DOI in the MCR along with associated hard switches located close to the RC&IS DOI (e.g. withdrawal and insertion pushbuttons) are the main interfaces for the operator to perform manual or semi-automatic control rod movements, activate (or deactivate) the RC&IS automatic rod movement mode, and activate and deactivate RC&IS bypass conditions. In addition, the operator can determine the details of the RC&IS status and related FMCRD status information at this same interface. Dedicated hard switches are also provided on the main control panel for manual initiation of an ARI function and for manual initiation of an SCRRI function. The ARI manual initiation switches interface directly with the Diverse Protection System (DPS) equipment, which provides associated signals to the NE-DCIS, which sends associated ARI motor run-in initiation signals to the RC&IS (also the DPS directly activates the ARI valves of the CRD system for accomplishing the hydraulic ARI function). The SCRRI manual initiation switches are within the scope of the RC&IS.

7.7.2.2.7.9 Reactor Operator Information

The RC&IS DOI provides the primary interface for the operator to access detailed RC&IS information (including details of the RC&IS status and related FMCRD status). RC&IS detection of abnormal conditions activates alarms so that the operator is notified in the change in RC&IS and/or FMCRD status.

In addition, the RC&IS provides FMCRD position information and summary RC&IS and FMCRD status information to the NE-DCIS equipment that provide for additional operator information to be displayed on other non-safety flat display panels in the MCR.

7.7.2.2.7.10 Setpoints

The RC&IS has no safety setpoints. The ATLM rod block setpoints are continuously calculated when the reactor power is above the low power setpoint. These setpoints also depend upon the last operating thermal limit information received from the NE-DCIS during an ATLM thermal limit update process. All other setpoints are established prior to plant startup operations and only adjusted, if needed, as a result of plant startup testing results. It is expected that none or very few of the RC&IS setpoints (besides the continual ATLM rod block setpoint updates) will require adjustment as a result of startup testing results.

7.7.2.3 Safety Evaluation

7.7.2.3.1 General Functional Requirements Conformance

The circuitry described for the RC&IS is completely independent of the circuitry controlling the scram valves. This separation of the scram and normal rod control functions prevents failures in the rod control and information circuitry from affecting the scram circuitry. The scram circuitry is discussed in Subsection 7.2.1. Because RC&IS directly controls movement of each control rod as an individual unit, a failure that results in inadvertent movement of a control rod affects only one control rod. The malfunctioning of any single control rod does not impair the effectiveness of a reactor scram. Therefore, no single failure in the RC&IS prevents a reactor scram. Repair, adjustment, or maintenance of the RC&IS components does not affect the scram circuitry.

Chapter 15 examines the various failure mode considerations for this system. The expected and abnormal transients and accident events analyzed envelope the failure modes associated with this system's components.

7.7.2.3.2 Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan for BWRs. The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Resolution of unresolved and generic safety issues for I&C is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C equipment in Tier 1.

General Design Criteria (GDC):

Criteria: GDC 13, 19, 24 and 29 apply.

Conformance: The RC&IS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

Regulatory Guides

In accordance with Table 7.1-1 and SRP Table 7-1, there are no regulatory guides applicable to the nonsafety-related RC&IS.

Branch Technical Positions (BTP)

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

The level of detail provided for the RC&IS within the Tier 1 and Tier 2 documents conforms to this BTP.

7.7.2.3.3 Environmental Considerations

The RC&IS is not required for safety purposes, nor is it required to operate after a design basis accident. This system is required to operate in the normal plant environmental conditions for the location of the RC&IS equipment (i.e. in back-panel area of the MCR and in clean areas of the Reactor Building).

7.7.2.4 Testing and Inspection Requirements

The RC&IS equipment is designed with consideration for online testing capabilities. The system can be maintained on line while repairs or replacement of hardware take place without causing any abnormal upset condition. The single-channel bypass capabilities support having continued RC&IS operation while repair or maintenance work is being performed on dual-channel scope of the RC&IS equipment.

7.7.2.5 Instrumentation Requirements

The CRD system is the RC&IS main direct interface to gather control rod position information and FMCRD status information and execute control rod movement commands. The FMCRD-related instrumentation that provides direct input to the RC&IS is addressed as part of the CRD system in Subsection 4.6.1. The primary output of the RC&IS is the three-phase power to the

FMCRD motors (and associated AC power to the motor built-in brakes) and the holding brakes of the CRD system to accomplish the RC&IS related rod movement functions.

The RC&IS modules that interface with FMCRD instrumentation include the appropriate signal conditioning and conversion components (e.g., resolver-to-digital converters, discrete contact closure or reed switch input circuitry, excitation power sources/supplies) for acquisition of the following:

- Resolver A and B position feedback signals (continuous signals);
- Coupling check (overtravel-out) position reed switch (discrete signal);
- Latched full-in and full-in position reed switches (discrete signal; these two reed switches are wired in parallel.)
- Buffer contact reed switch (discrete signal);
- Scram Timing position reed switches (discrete signals) at the following positions:
  - 0% insertion.
  - 10% insertion.
  - 40% insertion.
  - 60% insertion.
  - 100% insertion.

The induction motor controllers are designed to provide the proper three-phase power to the FMCRD motor (and power to the directly associated motor built-in brake) and the holding brakes of the CRD system to accomplish the RC&IS rod movement functions.

The RC&IS does not directly interface with any other basic plant instrumentation. The other inputs to the RC&IS come either by hardwired signal interfaces or by data communication links with other systems or from the RC&IS dedicated operator interface.

7.7.3 Feedwater Control System

7.7.3.1 Design Bases

Safety (10 CFR 50.2) Design Basis

The Feedwater Control System (FWCS) is not a safety-related system and is not required for safe shutdown of the plant. Therefore, the FWCS has no safety-related design basis.

Power Generation (Non-safety) Design Bases

The FWCS is designed such that the functional capabilities of safety-related systems are not inhibited.

The FWCS regulates the flow of feedwater into the reactor pressure vessel to maintain predetermined water level limits during transients and normal plant operating modes. The desired range of water level during normal power operation is based on steam separator performance. The requirements include limiting carryover, which can affect turbine performance, and limiting carryunder, which can affect overall plant efficiency.

If the water level rises to Level 8, then equipment protective action would trip the main turbine and reduce feedwater demand to zero. The feedwater pumps would trip if the water level continues to rise to Level 9. If the water level falls to Level 3, then the RPS would shut down the reactor. The RPS is a fully independent safety-related system (Subsection 7.2.1). If the water level continues to drop and reaches Level 2, the high-pressure make-up function of the CRD system would initiate. The CRD system is fully independent from other plant delivery or injection systems.

7.7.3.2 System Description

General Description

The FWCS is a power generation (control) system for the purpose of maintaining proper vessel water level in the operating range from high water level (Level 9) to low water level (Level 2). During normal operation, feedwater flow is delivered to the reactor vessel through three reactor feedpumps (RFPs), which operate in parallel. Each RFP is driven by an adjustable-speed, induction motor that is controlled by an adjustable speed drive (ASD). The fourth RFP is in standby mode and will auto-start if any operating feedpump trips while at power.

The FWCS is implemented on the triplicate, fault-tolerant digital controller (FTDC). The FTDC consists of three parallel processing channels, each containing the hardware and software for execution of the control algorithms. Each FTDC channel executes the control software for the control modes. At the operator's discretion, the system operation mode can be selected from the main control console. The functional diagram is provided as Figure 7.7-3.

During normal operation, the FWCS sends three speed demand signals (each of which reflects a voted FWCS processor output) to each feedpump adjustable speed drive (ASD). The ASD will perform a mid value vote and use it to control the speed/frequency of the feedpump motor. The mid value vote is also returned to FWCS as an analog input and compared to the speed demands sent by the FWCS. If an FTDC channel detects a discrepancy between the field voter output and the FTDC channel output, then a “lock-up” signal is sent to a “lock-up” voter and an alarm is activated in the control room.

Operation Modes

The following modes of feedwater flow control and thus level control are provided:

Single Element Control - At less than 25% of rated reactor powers, the FWCS uses single-element control based on vessel water level. In this mode the conditioned level error from the master level (proportional + integral, or PI) controller is used to determine the demand to either the low flow control valve (LFCV) or to an individual feedpump adjustable speed drive (ASD). The ASDs control feedpump motor speed and thus feedwater flow.

In addition, the FWCS can regulate the Reactor Water Cleanup/Shutdown Cooling (RWCU/SDC) system overboard control valve (OBCV) flow demand to counter the effects of density changes and purge flows into the reactor during heatup when steam flow is low.

Three-Element Control - During normal power range operation, the three-element control mode utilizes water level, total feedwater flow, total steam flow, and individual feedpump suction flow signals to determine the feedpump speed demand. The total feedwater flow is subtracted from the total steam flow signal to yield the vessel flow mismatch. The flow

mismatch signal is summed with the conditioned level error signal from the master level (PI) controller to provide the input signal for the master flow (PI) controller. The master flow controller provides the demand signal to the individual RFP loop trim controllers which use the suction flow signals to balance RFP flows. The trim controllers provide the speed demand signal to the ASDs, which control feedpump motor speed and thus feedwater flow.

Manual Feedpump Control - Each RFP can be controlled manually from the main control console through the FTDC by selecting the manual mode for that feedpump. In manual mode, the RFP speed demand signal that is sent directly to the ASD of the selected feedpump may be increased or decreased. Each feedpump is controlled manually at the manual/automatic transfer station.

Operational Considerations - The FWCS also provides interlocks and control functions to other systems. If the reactor water level reaches Level 8, then the FWCS simultaneously activates a control room alarm, and sends a zero-speed demand signal to the feedpump ASDs. At reactor water level setpoint level 8, the main turbine is tripped and at Level 9, a trip signal is sent to the feedwater pump ASD control breaker.

In addition, the FWCS initiates the signal to open the steam line condensate drain valves when steam flow falls below 40% of rated flow. Finally, the FWCS sends a zero-flow demand signal to the feedpump ASDs on identification of an ATWS condition.

7.7.3.3 Safety Evaluation

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C equipment in Tier 1.

General Design Criteria (GDC):

- Criteria: GDC 13, 19, and 24 apply.
- Conformance: The FWCS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

In accordance with the Regulatory Guide 1.151, “Instrument Sensing Lines,” the FWCS receives signals from sensors on vessel instrument lines in the Nuclear Boiler System. Refer to

Subsection 7.7.1.3 for a discussion of the criteria of RG 1.151 in relation to the Nuclear Boiler System.

The FWCS is not safety-related and is not required for safe shutdown of the plant. It is a power generation system for purposes of maintaining proper vessel water level. Its operation range is from high water level (Level 9) to low water level (Level 2). If the vessel level rises too high (Level 8), then the main turbine would trip and the feedpump ASD flow demand would reduce to zero. Continued rising water level to Level 9 would result in a trip of all ASD feedpumps. The vessel water level rising to Level 8 or falling to Level 3 would result in the shutdown of the reactor by the RPS. Refer to Subsection 7.2.1 for RPS description.

Branch Technical Positions (BTP)

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

The level of detail provided in Tier 1 and Tier 2 documents conforms to this BTP.

7.7.3.4 Testing and Inspection Requirements

The FTDC self-test and on-line diagnostic test features are capable of identifying and isolating failures of process sensors, I/O cards, power buses, power supplies, processors and inter-processor communication paths. These features can identify the presence of a fault and determine the location of the failure down to the module level.

The FWCS components and critical components of interfacing systems are tested to assure that specified performance requirements are satisfied. Preoperational testing of the FWCS is performed before fuel loading and startup testing to assure that the system functions as designed and that stated system performance is within specified criteria.

7.7.3.5 Instrumentation Requirements

Power Sources

Redundant uninterruptible power supplies (UPS) power the FWCS digital controllers and process measurement equipment. No single power source or single power supply failure results in the loss of FWCS functions.

Equipment

The FWCS consists of the following elements:

- The FTDC that contains the software and processors for execution of the control algorithms.
- Feedwater flow signals that provide for the measurement of the total flow rate of feedwater into the vessel.
- Steam flow signals that provide for the measurement of the total flow rate of steam leaving the vessel.
- Feedpump suction flow signals (discharge flow may be substituted) that provide for the measurement of the suction flow rate of each feedpump.

- The LFCV differential pressure transmitters that provide for the measurement of the pressure drop across the LFCV, for LFCV gain control.
- The LFCV flow transmitters that provide for the measurement of the flow through the LFCV, for both LFCV control and low thermal power calculations.

Reactor Vessel Water Level Measurement

Reactor vessel narrow-range water level is measured by at least three identical, independent sensing systems. For each level measurement channel, a differential pressure transmitter senses the difference between the pressure caused by a constant reference column of water and the pressure caused by the variable height of water in the reactor vessel. The differential pressure transmitters are part of the Nuclear Boiler System. (Refer to Subsection 7.7.1.2 for a description of the reactor vessel instrumentation.) The FWCS FTDC determines one validated narrow-range level signal using the multiple level measurements as inputs to a signal validation algorithm. The validated narrow-range water level is indicated on the main control console in the control room.

Steam Flow Measurement

The steam flow in each of four main steam lines is sensed at each reactor pressure vessel nozzle venturi that is part of the Nuclear Boiler System. (Refer to Subsection 7.7.1.2 for a description of the reactor vessel instrumentation.) Two flow transmitters per steam line, which are part of the FWCS, sense the venturi differential pressure and send these signals to the FTDC through the multiplexing function of NE-DCIS. The FWCS multiplexing function signal-conditioning algorithms take the square root of the venturi differential pressures and provide eight steam flow rate signals, two for each steam line, to the FTDC for validation. These validated steam line flow measurements are summed in the FTDC to give the total steam flow rate out of the vessel. The total steam flow rate is indicated on the main control console in the control room.

Feedwater Flow Measurement

Feedwater flow is sensed at a single flow element in each of the two feedwater lines, which are part of the Condensate and Feedwater System. Three transmitters per feedwater line, which are part of the FWCS, sense the differential pressure and send these signals to the FTDC through the NE-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide six feedwater flow rate signals, three for each feedwater line, to the FTDC for validation. These validated feedwater line flow measurements are summed in the FTDC to give the total feedwater flow rate into the vessel. The total feedwater flow rate is indicated on the main control console in the control room.

Feedpump suction flow is sensed at a single flow element, which is part of the Condensate and Feedwater System, upstream of each feedpump. The suction line flow element differential pressure is sensed by a single transmitter, which is part of the FWCS, and sent to the FTDC through the NE-DCIS multiplexing function. The FWCS multiplexing function signal conditioning algorithms take the square root of the differential pressure and provide the suction flow rate measurements to the FTDC. The feedpump suction flow rate is compared to the demand flow for that pump and the resulting error is used to adjust the speed demand to the ASD to reduce that error and balance RFP flow between operating pumps.

7.7.4 Plant Automation System

7.7.4.1 Design Bases

Safety (10 CFR 50.2) Design Basis

Plant Automation System (PAS) has no safety-related design basis. However, this system is designed in such a manner that the functional capabilities of safety-related systems are not obviated. Abnormal events requiring control rod scrams are sensed and controlled by the safety-related Reactor Protection System (RPS), which is fully independent of Plant Automation System. Discussions on RPS are provided in Subsection 7.2.1.

This system provides the capability for supervisory control of the entire plant by supplying set-point commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate.

Power Generation (Non-Safety) Design Bases

The bases of this system are to provide supervisory control to regulate reactivity during criticality control, provide heatup and pressurization control, regulate reactor power, control turbine/generator output, control secondary nonsafety-related systems and provide reactor startup / shutdown controls.

7.7.4.2 System Description

The primary purpose of the PAS is for reactivity control, heatup and pressurization control, reactor power control, generator power control (MWe control) and plant shutdown control. The PAS consists of redundant, triplicate process controllers. The functions of the PAS are accomplished by suitable algorithms for different phases of reactor operation which include approach to criticality, heatup, reactor power increase, automatic load following, reactor power decrease, and shutdown. The Plant Automation System receives input from the Neutron Monitoring System (Subsection 7.2.2), Non-Essential Distributed Control and Information System (Subsection 7.9.2), and the Steam Bypass and Pressure Control System (Subsection 7.7.5). The output demand request signals from the Plant Automation System are to the Rod Control and Information System to position the control rods, to the Steam Bypass and Pressure Control System for pressure setpoints, and to the Turbine Control System for load following operation. A simplified functional block diagram of the PAS is provided in Figure 7.7-4.

The PAS interfaces with the operator's console to perform its designed functions. From the operator's control console for automatic plant startup, power operation, and shutdown functions, the operator uses PAS to issue supervisory control commands to nonsafety-related systems, and adjusts set-points of lower level controllers to support automation of the normal plant startup, shutdown, and power range operations. In the automatic mode, the PAS also issues command signals to the turbine master controller, which contains appropriate algorithms for automated sequences of turbine and related auxiliary systems. This control console consists of a series of break point controls for a prescribed plant operation sequence. When all the prerequisites are satisfied for a prescribed breakpoint in a control sequence, a permissive is requested and upon operator acceptance, the prescribed control sequence is initiated or continued. The PAS then initiates demand signals to various system controllers to carry out the predefined control

functions. For non-automated operations that are required during normal startup or shutdown (e.g., change of reactor mode switch status), automatic prompts are provided. Automated operations continue after the prompted actions are completed manually. The functions associated with reactor power control are performed by the PAS.

For reactor power control, the PAS contains algorithms that can change reactor power by control rod motions. A prescribed control rod sequence is followed when manipulating control rods for reactor criticality, heatup, power changes, and automatic load following. Each of these functions has its own algorithm to achieve its designed objective. During automatic load following operation, the PAS interfaces with the Turbine Control System to coordinate main turbine and reactor power changes for stable operation and performance.

The normal mode of operation of the PAS is automatic. If any system or component conditions are abnormal during execution of the prescribed sequences, the PAS would automatically switch into the manual mode, any operation in progress would stop, and alarms would activate. With the PAS in manual mode, the operator can manipulate control rods through the normal controls. A failure of the PAS would not prevent manual control of reactor power, and would not prevent safe shutdown of the reactor.

The triplicate fault-tolerant digital controllers (FTDC), and redundant system controllers perform the PAS control functional logic

7.7.4.3 Safety Evaluation

Plant Automation System does not perform or ensure any safety-related function. This system is designed such that functionalities of safety-related systems in the plant are not affected by it.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Resolution of unresolved and generic safety issues for I&C is discussed in Subsection 7.1.2.2.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C equipment in Tier 1.

General Design Criteria (GDC):

- Criteria: GDC 13, 19, and 24 apply.

Conformance: The PAS complies with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

Branch Technical Positions (BTP):

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

The level of detail provided herein for the Plant Automation System conforms to this BTP.

7.7.4.4 Testing And Inspection Requirement

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, FTDC is equipped with self-test and on-line diagnostic capabilities for identifying and isolating failure of input/output signals, buses, power supplies, processors, and inter-processor communications. These on-line tests and diagnostics can be performed without interrupting the normal control operation of the PAS.

7.7.4.5 Instrumentation Requirements

The instrumentation required for the system can be categorized as (1) control room instrumentation, needed for man-machine interface, (2) hardware and software for input/output interfaces and controller functions, and (3) direct non multiplexed sensor inputs, needed by the system. The control room instrumentation supporting this system would be consistent with the control room design. The PAS consists of triplicate master controllers and duplicated system controllers as hardware, and required software for controller functions and input/output interfaces.

7.7.5 Steam Bypass and Pressure Control System

7.7.5.1 Design Bases

Safety (10 CFR 50.2) Design Basis

The Steam Bypass and Pressure Control (SB&PC) system does not perform or ensure any safety-related function, is classified as a nonsafety-related system, and has no safety-related design basis.

Power Generation (Non-safety) Design Bases

The SB&PC system is designed such that the functional capabilities of safety-related systems are not inhibited.

The SB&PC system is essential to the power generation cycle in that SB&PC controls reactor pressure during plant startup, power generation, and shutdown modes of operation.

The design objective is to enable a fast and stable response to pressure and system disturbances, and to pressure setpoint changes over the operating range using turbine control valves (TCVs) and turbine bypass valves (TBVs) for controlling reactor pressure. In addition, the design objective of the steam bypass system is to discharge reactor steam directly to the main condenser in order to regulate reactor pressure whenever the turbine cannot utilize all of the steam generated by the reactor.

7.7.5.2 System Description

General Description

The purpose of the SB&PC system is to control reactor pressure during plant startup, power generation, and shutdown modes of operation. This is accomplished through control of the turbine control valves (TCVs) and turbine bypass valves (TBVs), such that susceptibility to reactor trip, turbine-generator trip, main steam isolation, and safety/relief valve opening is

minimized. Triplicate fault tolerant digital controllers (FTDC) using feedback signals from reactor vessel dome pressure sensors generate command signals for the TBVs and pressure regulation demand signals used by the Turbine Control system (TCS) to generate demand signals for the TCVs. For normal operation, the TCVs regulate reactor pressure. However, whenever the total steam flow demand from the SB&PC system exceeds the effective turbine control valve steam flow demand, the SB&PC system sends the excess steam flow directly to the main condenser through the TBVs.

The ability of the plant to load follow the grid-system demands is accomplished by the aid of control rod actions. In response to the resulting steam production demand changes, the Steam Bypass and Pressure Control (SB&PC) system adjusts the demand signals sent to the TCS so that the TCS adjusts the TCVs to accept the control steam output change, thereby controlling pressure.

Controls and valves are designed such that steam flow is shut off upon loss of control system electrical power or hydraulic system pressure.

Refer to Figure 7.7-5, SB&PC Simplified Functional Block Diagram, and Figure 7.7-6, SB&PC Fault Tolerant Digital Controller (FTDC) Block Diagram, for overview of functions and interfaces.

Normal Plant Operation

At steady-state plant operation, the SB&PC system maintains reactor vessel pressure at a nearly constant value, to ensure optimum plant performance. During normal operational plant maneuvers (pressure setpoint changes, level setpoint changes), the SB&PC system provides responsive, stable performance to minimize vessel water level and neutron flux transients. During plant startup and heatup, the SB&PC system provides for automatic control of the reactor pressure. Independent control of reactor pressure and power is permitted during reactor-vessel heatup, by varying turbine bypass flow as the main turbine is brought up to speed and synchronized. The SB&PC system also controls pressure during normal (main steam isolation valves open) reactor shutdown to control the reactor cooling rate.

Abnormal Plant Operation

Events leading to reactor trip present significant transients during which the SB&PC system maintains reactor pressure. These transients are characterized by large variations in steam flow and core thermal power output, which affect reactor water level. The SB&PC system is designed to stabilize system pressure and thus aid the feedwater/level control systems in maintaining reactor water level.

The SB&PC system is also designed for operation with other reactor control systems to avoid reactor trip after significant plant disturbances. Examples of such disturbances are loss of one feedwater pump, inadvertent opening of safety/relief valves or TBVs, main turbine stop/control valve surveillance testing, and steam line isolation valves testing.

The SB&PC inhibits opening of the TBVs upon detection of high condenser pressure, for condenser protection.

Operational Considerations

Manually operated provisions permit opening of the main steam lines (up to the steam bypass valves and turbine stop valves) before normal condenser vacuum is obtained and permits cold shutdown testing of the isolation valves. The SB&PC system allows remote manual bypass operation in the normal opening sequence during plant start up and shut down. This facilitates purge of the vessel and main steam lines of accumulated noncondensable gases early on in the start-up process, and controls the rate of cooling during reactor shutdown to atmospheric pressures. Upon increasing pressure transients during such manual operation, the controls provide automatic override of the manual demand signal by the normal bypass demand. The system automatically returns to the manual demand signal when pressure transient causing the increased bypass demand is relieved.

Triplicate microprocessor-based FTDC performs the SB&PC system functional logic and process control functions. Because of the triple redundancy, it is possible to lose one complete processing channel without affecting the system function. This also facilitates taking one channel out of service for maintenance or repair while the system is on-line.

During operation of the SB&PC, the operator may observe the performance of the plant via flat display panels on the main control console or on large screen displays in the MCR. As described in Subsection 7.7.5.5 below, the on-line diagnostic provision assures that all detections of transducer/controller failures are indicated to the operator and maintenance personnel. The triplicate logic facilitates on line repair of the controller circuit boards. During abnormal conditions that result in high condenser pressure, the steam bypass valves and MSIVs close to prevent positive pressure conditions that would open the main condenser rupture disks. Manually operated provisions permit opening of the MSIVs (i.e., inhibit the closure function) during startup operation. This vacuum protection function bypass permits heatup of the main steamlines (up to the steam bypass valves and turbine stop valves) before normal main condenser vacuum is obtained. The bypass also permits cold shutdown testing of the isolation valves.

Any plant or component condition that inhibits bypass valve opening is alarmed in the MCR and must be manually reset by the operator.

The SB&PC has no safety setpoints because it is not a safety-related system. Actual operational setpoints will be determined during startup testing.

Redundant uninterruptible non-Class 1E power supplies and sources power the SB&PC system controls and bypass valves. No single power failure results in the loss of any SB&PC system function. Upon detection of a failure of two or more channels in the controller, a turbine trip is initiated.

The pressure control function provides automatic load following by forcing the turbine control valves to remain under pressure control supervision, while enabling fast bypass opening for transient events requiring fast reduction in turbine steam flow.

The steam bypass function controls reactor pressure by modulating automatically operated, regulating bypass valves in response to the bypass flow demand signal. This control mode is assumed under the following conditions:

- During reactor vessel heatup to rated pressure;

- While the turbine is brought up to speed and synchronized;
- During power operation when reactor steam generation exceeds the turbine steam flow requirements;
- During plant load rejection and turbine/generator trips; and
- During cooldown of the nuclear boiler.

7.7.5.3 Safety Evaluation

The SB&PC system is classified as primary power generation system and is not required for safety purposes, nor is it required to operate during or after any design basis accidents. The system is required to operate in the normal plant environment and is essential to the power production cycle. The SB&PC equipment is located in the main control room area of the control building and is subject to the environment of that area. The SB&PC FTDC panel and components within are designed for retaining structural integrity as to not impair any safety-related equipment in its area from performing its safety function.

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with Section 7.7 of the Standard Review Plan. The following analysis lists the applicable criteria, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR Part 52

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Conformance: SB&PC system is nonsafety-related and conforms in that there are no unresolved issues for the SB&PC system. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: Test, inspection, analyses, and acceptance criteria of the SB&PC FTDC are identified in Tier 1.

52.47(a)(1)(vii) Interface Requirements

Conformance: Design interface requirements during the licensing certification and design phases shall be commensurate with the detail required to support the completion of the final safety analysis and design-specific probabilistic risk assessment. Interface material is provided in Tier 1.

52.79(c) ITAAC in Combined Operating License Applications

Conformance: SB&PC system is nonsafety-related and conforms to those sections applicable for test, inspection, analyses, and acceptance criteria of the SB&PC FTDC, as identified in Tier 1.

General Design Criteria

Criteria: GDC 13, 19, and 24

Conformance: The SB&PC is in conformance with the GDC identified above. Refer to Subsection 3.1.2 for general discussion of the GDC.

Regulatory Guides

Regulatory Guide 1.151, Instrument Sensing Lines

Conformance: Not applicable to the SB&PC system. The SB&PC receives reactor dome pressure signals from sensors in the Nuclear Boiler System. Refer to Subsection 7.7.1.3 for discussion of the criteria of R.G. 1.151 in relation to the Nuclear Boiler System. SB&PC also receives condenser absolute pressure signals form sensors in the Main Condenser and Auxiliaries System.

Branch Technical Positions

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

Conformance: The level of detail is commensurate with this BTP.

7.7.5.4 Testing and Inspection Requirements

The FTDC input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, FTDC is equipped with on-line diagnostic capabilities for identifying and isolating failure of input/output signals, buses, power supplies, processors, and inter-processor (IO Net) communications. These on-line diagnostics can be performed without interrupting the normal control operation of the SB&PC system.

The SB&PC components and critical components of interfacing systems are tested to assure that the specified performance requirements are satisfied. Preoperational testing of the SB&PC is performed before fuel loading and startup testing to assure that the system functions as designed and that stated system performance is within specified criteria.

7.7.5.5 Instrumentation Requirement

7.7.5.5.1 Power Sources

Uninterruptible Nonsafety AC Power Supply

The nonsafety inverters of the uninterruptible power source are normally supported by AC power. However, if off-site power fails, it receives power from DC source (batteries). SB&PC has three redundant nonsafety AC uninterruptible power supplies of 120 ±10% volt AC, 60 Hz. SB&PC panel design is such that loss of one power supply or incoming power source shall not affect SB&PC system functional operation and thus plant operation.

Lighting and Service Power System (LSP)

LSP supplies 120 VAC to SB&PC for lighting and maintenance equipment.

7.7.5.6 Major instrument interfaces with SB&PC

Nuclear Boiler System (NBS)

NBS provides narrow range dome pressure, wide range dome pressure, inboard MSIV position, and outboard MSIV position signals to SB&PC. TBVs interface with NBS to receive main steam supply.

Rod Control and Information System (RC&IS)

SB&PC sends reactor dome pressure signals to RC&IS.

Feedwater Control System (FWCS)

SB&PC sends reactor dome pressure signals to FWCS.

Plant Automation System (PAS)- Automatic Power Regulator (APR)

SB&PC supplies the following signals to PAS-APR:

- SB&PC Auto/OK status signals
- Operating pressure setpoint signals
- Total (average) TBV position signals
- Pressure regulator output signals
- Limited speed regulator output signals
- Load reference signals
- Wide range and narrow range dome pressure signals
- First TBV position signals

PAS-APR outputs the following signals to SB&PC:

- AFC status signals
- Signals to raise pressure setpoint
- Signals to lower pressure setpoint
- PAS-APR fatal fault signals
- Reactor Thermal Power Signals

NE-DCIS - Plant Computer Function (PCF)

The Performance Monitoring and Control Function (PMCF) of PCF within NE-DCIS receives signals from SB&PC for performance monitoring.

NE-DCIS - Multiplexing

The Multiplexing function of NE-DCIS provides the distributed control and instrumentation data communications network to support the monitoring and control of interfacing plant systems.

Remote multiplexing units (RMUs) are located throughout the plant to support SB&PC and its interfaces with other systems.

Main Control Room Panels (MCRP)

The MCRP operator interface within NE-DCIS contains controls needed for SB&PC operation and displays variables and alarms from SB&PC.

Main Control Room Back Panels (MCRBP)

The SB&PC's triple-redundant FTDC panel is mounted in a MCRBP.

Turbine Bypass System (TBS)

TBS provides temperature signals to SB&PC from thermocouples installed in each TBV discharge pipe, located between TBV and condenser, for bypass steam leakage detection.

Main Turbine (MT)

SB&PC sends the following signals to the Main Turbine:

- Signals to trip the turbine

Main Turbine provides the following signals to SB&PC:

- Turbine trip signals

Turbine Control System (TCS) - Electro-Hydraulic Control (EHC)

SB&PC sends the following signals to TCS-EHC:

- Pressure regulation demand signals

TCS - EHC provides the following signals to SB&PC:

- Turbine speed regulator output signals
- Load reference signals
- Turbine steam flow demand signals
- Turbine first stage pressure signals
- PLU (Power-Load Unbalance) event signals
- TCS - EHC CPU failure signals

Main Condenser and Auxiliaries

The main condenser receives steam from TBVs. The Main condense provides condenser narrow and wide range pressure signals, from all shells of the condenser, to SB&PC.

Auxiliary Boiler (AUXB)

SB&PC sends signals to start the electric auxiliary boiler or increase its steam production rate upon MSIV closure condition. From the foregoing analysis, it is concluded that the SB&PC meets its design bases.

7.7.6 Neutron Monitoring System - Nonsafety-Related Subsystems

7.7.6.1 Design Basis

Safety (10 CFR 50.2) Design Basis

AFIP and MRBM

The Neutron Monitoring System has two nonsafety-related subsystems, the Automated Fixed In-Core Probe (AFIP) subsystem and the Multi-Channel Rod Block Monitor (MRBM) subsystem. Neither the AFIP subsystem nor MRBM performs or ensures any safety-related function, and thus, the AFIP and MBRM subsystems have no safety design basis.

Power Generation (Non-Safety) Design Bases

AFIP

The AFIP has the following power generation design bases:

- Provide a signal proportional to the axial neutron flux distribution at the radial core locations of the LPRM detectors. This signal allows calibration of LPRM;
- Provide sufficient axial neutron flux monitoring with corresponding axial position and indication to allow point-wise measurement of the axial neutron flux distribution to support the determination of three-dimension core power distribution; and
- Provide a totally automated mode of LPRM calibration by direct interface with the plant computer function of the NE-DCIS.

MRBM

The MRBM has the following power generation design bases:

- Provide a signal to RCIS to block rod movement if the MRBM signal exceeds a preset rod block setpoint to prevent fuel damage;
- Provide MRBM values to the NE-DCIS;
- Provide bypass capability of one out of two MRBM channels;
- Provide bypass of individual LPRM channels in its calculations;
- Provide online test and diagnostic capability to validate proper operation of its microprocessor-based system; and
- Provide rod block status to the main control room alarm system.

7.7.6.2 System Description

AFIP

General Description

The AFIP subsystem is comprised of AFIP sensors and their associated cables, as well as the signal processing electronic unit. The AFIP sensors are gamma thermometer in design. The AFIP gamma thermometer sensors are installed permanently within the LPRM assemblies. In each LPRM assembly in the core, there are four AFIP gamma thermometer sensors evenly

distributed across the LPRM assembly, with one gamma thermometer installed next to each LPRM detector. Consequently, there are AFIP sensors at all LPRM locations. The AFIP sensor cables are routed within the LPRM assembly and then out of the reactor pressure vessel through the LPRM assembly penetration to the vessel. The AFIP subsystem generates signals proportional to the axial power distribution at the radial core locations of the LPRM detector assemblies. The AFIP signal range is sufficiently wide to accommodate the corresponding local power range that covers from approximately 1% to 125% of reactor rated power.

During core power and LPRM calibration, the AFIP signals are collected automatically to the AFIP data processing and control unit, where the data are properly amplified and compensated by applying correct sensor calibration adjustment factors. Such data are then sent to the plant computer function of the NE-DCIS for core local power and thermal limits calculations. The calculated local power data are then used subsequently for LPRM calibration. The AFIP data collection and processing sequences are fully automated, with manual control available.

The AFIP gamma thermometer sensor has near constant, very stable detector sensitivity due to its operation principle, and its sensitivity does not depend upon fissile material depletion or radiation exposure. The AFIP gamma thermometer, however, can be calibrated, either manually or automatically, by using a built-in calibration device inside the gamma thermometer/LPRM assembly. The calibrated new sensitivity data of the AFIP sensors are stored in the AFIP control unit and are readily applied to the newly collected AFIP data to provide accurate local power information. The interval of the gamma thermometer calibration is to be specified in the plant technical specification.

With its stable sensitivity and rugged hardware design, the AFIP sensor has a lifetime much longer than that of the LPRM detectors. The AFIP sensors in an LPRM assembly are replaced together with the LPRM detectors when the whole LPRM assembly is replaced. The AFIP detectors within the LPRM assembly are installed such that physical separation is maintained between the LPRM detectors and the AFIP detectors. The AFIP cables are also routed separately within the LPRM assembly from the LPRM detector cables, with separate external connectors. More descriptions of the AFIP is included in Appendix 7A and in Reference 7.7-1.

Classification

The AFIP is nonsafety-related. It is an operational subsystem and has no safety-related function.

Power Supply

The power for the AFIP calibration heaters is supplied from the nonsafety-related instrument 120VAC Instrument and Control (ICP) power source; the power for the AFIP logic is supplied from redundant nonsafety-related instrument 120VAC uninterruptible power sources.

Environmental Considerations

The AFIP sensor meets BWR environmental requirements. The connectors and cabling located in the drywell are designed for continuous duty (see Appendix 3D). The AFIP instruments are designed to operate under the expected environmental conditions in the areas it resides.

Operational Considerations

The AFIP is operated during reactor operation to provide local power information for three-dimensional power calculation and for calibration of the LPRM channels. The AFIP operation is

fully automated including AFIP data collection, AFIP sensor calibration, AFIP data amplification, and data transfer to the plant computer. Manual operation capability is available. The subsystem has no safety setpoints.

MRBM

General Description

The MRBM Subsystem logic issues a rod block signal that is used in the RCIS logic to enforce rod blocks that prevent fuel damage by assuring that the minimum critical power ratio (MCPR) and maximum linear heat generation rate (MLHGR) do not violate fuel thermal safety limits. Once a rod block is initiated, manual action is required by the operator to reset the system.

The MRBM microcomputer-based logic receives input signals from the LPRMs and the APRMs of the NMS. It also receives control rod status data from the rod action and position information subsystem of the Rod Control and Information System (RC&IS) to determine when rod withdrawal blocks are required. The MRBM uses the LPRM signals to detect local power change during the rod withdrawal. If the MRBM signal, which is based on averaged LPRM signal, exceeds a preset rod block setpoint, a control rod block demand will be issued. The MRBM monitors the core in 4-by-4 fuel bundle regions in which control rods are being withdrawn. The MRBM algorithm covers the monitoring of multiple regions simultaneously depending upon the size of the gang of rods being withdrawn. Because it monitors more than one region at any one time, it is called the multi-channel rod block monitor. The MRBM is a dual channel system, but not classified as a safety system.

Classification

The MRBM is nonsafety-related. Its activating interface is through the RC&IS, which is also a nonsafety-related system.

Power Supply

The power supply for the MRBM is from the non-divisional (nonsafety-related) 120 VAC uninterruptible buses (in two different load groups).

Environmental Considerations

The MRBM is located in the MCR. It is physically and electrically isolated from the safety NMS subsystems. All interfaces with the safety NMS subsystems are via optical isolation.

7.7.6.3 Safety Evaluation

Table 7.1-1 identifies the nonsafety-related control systems and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the applicable criteria and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

Unresolved and generic safety issues are discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi), ITAAC in Design Certification Applications

ITAAC are provided for the I&C equipment in Tier 1.

10 CFR 52.47(a)(1)(vii), Interface Requirements

Interface material is provided in Tier 1.

10 CFR 52.79(c), ITAAC in Combined License Applications

ITAAC are provided for the I&C equipment in Tier 1.

General Design Criteria (GDC):

- Criteria: GDC 13, 19, and 24 apply.
- Conformance: The AFIP and MRBM subsystems are in compliance with these GDC. Refer to Subsection 3.1.2 for a general discussion of the GDC.

Branch Technical Positions (BTP)

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

The level of detail provided in Tier 1 and Tier 2 documents conforms to this BTP.

7.7.6.4 Testing And Inspection Requirements

AFIP

The AFIP instrument (not including sensors) is designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access to the service personnel.

The AFIP sensor is testable and able to be calibrated for its sensitivity. The AFIP instrument unit includes an algorithm that can automatically detect and reject failed AFIP sensor signals. It also includes a logic that can verify proper communication with the plant computer of the NE-DCIS system.

The duration for AFIP testing and calibration is based on the applicable NMS AFIP design document and the instruction manual of the AFIP subsystem, or plant technical specification.

MRBM

The MRBM subsystem is designed such that they can be tested, inspected, and calibrated as required during plant operation without causing plant shutdown or scram, and with easy access to the service personnel.

It also includes a logic that can verify proper communication with the NE-DCIS system.

The duration for MRBM testing and calibration is based on the applicable NMS MRBM design document and the instruction manual of the MRBM subsystem.

7.7.6.5 Instrumentation Requirements

AFIP

The AFIP instrument is based on the digital measurement and control design practices that use digital design concepts and include microprocessor-based programmable and memory units.

The AFIP instrument follows a modular design concept such that each modular unit or its subunit is replaceable upon repair service.

The instrument has a flexible interface design to accommodate either metal wire or fiber-optic communication links.

The AFIP instrument is provided with necessary operator-interface functions based on adequate NMS man-machine interface requirements.

Basic Control Logic Requirements—The AFIP includes basic logics such as periodic demand for sensor calibration and data collection, as well as logic as part of the communication protocol with the plant computer function.

Basic Instrument Arrangement Requirements—The AFIP instrument cabinets are located in appropriate areas of the reactor building with physical and electrical separation from the safety-related NMS instruments, and with acceptable environmental conditions.

MRBM

The MRBM subsystem is based on the digital measurement and control design practices that use digital design concepts and include microprocessor-based programmable and memory units. The MRBM follows a modular design concept such that each modular unit or its subunit is replaceable upon repair service. The MRBM has a flexible interface design to accommodate either metal wire or fiber-optic communication links. The MRBM instrument is provided with necessary operator-interface functions based on adequate NMS man-machine interface requirements.

Basic Control Logic Requirements—The MRBM includes basic logics such as continuous LPRM data collection, MRBM rod block algorithm calculation, MRBM setpoint comparison, and communication protocol with the NE-DCIS.

Basic Instrument Arrangement Requirements—The MRBM subsystem is located within the nonsafety equipment rooms of the control building with appropriate physical and electrical separation from the safety-related NMS instruments, and with acceptable environmental conditions.

7.7.7 Containment Inerting System

7.7.7.1 Design Bases

The Containment Inerting System (CIS) design bases are discussed in Subsection 9.4.9.

7.7.7.2 System Description

The CIS system description is discussed in Subsection 9.4.9.2.

7.7.7.3 Safety Evaluation

CIS is nonsafety-related except for the containment isolation function. Failure of the nonsafety-related components would not adversely affect any safety-related system.

Evaluation Against Regulatory Requirements

In accordance with Table 7.1-1, and SRP Section 7.7, the following criteria are addressed:

10 CFR 52.47 and 52.79

- 52.47(a)(1)(iv), Resolution of Unresolved and Generic Safety Issues

  Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

- 52.47(a)(1)(vi), ITAAC in Design Certification Applications

  Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

- 52.47(a)(1)(vii), Interface Requirements

  Conformance: Interface material is provided in Tier 1.

- 52.79(c), ITAAC in Combined License Applications

  Conformance: ITAAC are provided for I&C systems and equipment in Tier 1.

General Design Criteria

CIS meets the requirements of GDC 13, 19, and 24. Control and instrumentation is provided to operate the system, monitor process variables during startup, normal, and abnormal reactor operation. The CIS is operable from the main control room.

Regulatory Guides

In accordance with Table 7.1-1, there are no regulatory guides directly applicable to the nonsafety-related CIS. However, the CIS instrument lines penetrating containment meet the requirements of Regulatory Guides 1.11 and 1.151. Sensing lines are Seismic Category I Quality Group B and are provided with redundant isolation valves that can be isolated locally or remote manually from the main control room.

Branch Technical Positions

In accordance with Table 7.1-1, only BTP HICB-16, Guidance on the Level of Detail Required for Design Certification Applications Under 10 CFR Part 52, is applicable to the nonsafety-related CIS. The level of detail provided for CIS within the Tier 1 and Tier 2 documents is in conformance with this BTP.

7.7.7.4 Testing and Inspection Requirements

The CIS testing and inspection requirements are discussed in Subsection 9.4.9.

7.7.7.5 Instrumentation Requirements

Logic and Interlocks

The CIS operation is remote manually or automatically activated from the main control room by aligning corresponding valves through remote manual control switches.

During inerting mode, once the steam-heated vaporizer has been activated, a temperature controller accomplishes automatic control of the steam supply. A temperature sensor at the outlet of the steam vaporizer provides input to the temperature controller that then regulates the amount of steam. Low nitrogen temperature in the steam vaporizer outlet sounds an alarm and

low-low temperature condition shuts off the main inerting line. The auxiliary steam supply is manually terminated.

When the required inert containment pressure is reached, the CIS drywell pressure switch provides signal to isolate the nitrogen supply shutoff valve.

Upon completion of the initial inerting, CIS is manually or automatically aligned to make-up mode. Make up is accomplished by the automatic modulation of the pressure control valve provided to make-up nitrogen. The opening and closing of the pressure control valve is driven by the pressure controller in response to change of containment pressure.

Make-up nitrogen supply is vaporized and heated up to appropriate temperature by an electric heater. The electric heater is manually loaded to its power source. Once activated, it continues to operate in automatic on-off mode until manually disconnected. Temperature sensors provide switching signals to start-stop the heater. When the required temperature is reached, heater automatically cuts off electrical power feed into the heater elements.

The de-inerting process is manually or automatically activated, by aligning CIS to the Reactor Building HVAC to rid resident gases in the containment with breathable air supplied by the Reactor Building HVAC.

During primary containment isolation events, CIS primary containment isolation valves automatically close upon receipt of isolation signal from Leak Detection and Isolation System. Details of the isolation logic are discussed in Subsection 7.3.2.

The CIS is capable of providing continued nitrogen makeup during isolation events. This is accomplished by overriding the isolation signal to the makeup isolation valves with controlled bypass switches.

A simplified system diagram is shown in Figure 9.4-13.

Instrumentation and Control

Drywell pressure sensors, part of the Containment Monitoring System (CMS), are provided for monitoring containment pressure. These instruments provide input to the pressure controller to control makeup flow and provide alarm signals on a high drywell pressure condition.

Permanently installed temperature and humidity sensors are provided in several locations and elevations inside containment. These sensors are fed to the plant computer function for averaging and continuous monitoring of the containment.

Oxygen analyzers are provided to monitor oxygen levels in the containment during startup, normal, and abnormal plant operating conditions. Two sample points in each compartment (i.e., upper drywell area, lower drywell area, wetwell air space) are provided (one in a high and one in a low location) on opposite sides of the compartment. Each air lock is also sampled. Oxygen levels in the CIS exhaust line are also monitored. A high oxygen level indication is alarmed in the main control room.

A flow-metering device is installed in the makeup line to monitor the amount of nitrogen make up injected into the containment. Total nitrogen make-up flow (make-up flow to containment and make-up flow to the High Pressure Nitrogen Supply System (HPNSS) are also monitored. Total nitrogen flow indicates total containment atmosphere leakage during normal plant operation. Excessive leakage is alarmed in the main control room.

Separate flow metering devices are also provided to both drywell and wetwell inerting and de-inerting flows.

The CIS is described in Section 9.4.

Alarms and Indications

The following alarms and indications are also provided in the main control room:

- High drywell pressure;
- High makeup flow;
- Excessive or gross containment leakage;
- High and low make-up flow temperature;
- High and low electric heater temperature;
- Low main vaporizer outlet temperature;
- Low nitrogen storage tank level;
- Keylock switch in Override position;
- High oxygen level;
- Wetwell pressure indication;
- Valve position switch status indication;
- Pilot solenoid status indication;
- Drywell temperature; and
- Wetwell temperature.

7.7.8 COL Information

None.

7.7.9 References

7.7-1 GE Energy Nuclear, "Gamma Thermometer System for LPRM Calibration and Power Shape Monitoring," NEDC-33197P, Class III (GE proprietary), July 2005.

Table 7.7-1

Automatic Power Regulator Interfaces

APR Functions	Input Signals	Output Signals
Criticality Control	1. SRNM output (NMS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Criticality / subcriticality validation check (plant computer function)
Heatup & Pressurization	1. SRNM output (NMS) 2. Reactor water temperature (PGCS) 3. Reactor heatup schedule (Plant Computer Function) 4. Reactor mode (PGCS) 5. Dome Pressure (SB&PC)	1. CR control demand (RC&IS) 2. SB&PC pressure setpoint
Reactor Power Control	1. Target generator power (PGCS) 2. Pressure controller output (equivalent load) (SB&PC) 3. Load demand change (SB&PC) 4. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TCS)
Generator Power Control	1. Generator power feedback signal (PGCS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. Load demand (TCS)
Reactor Shutdown Control	1. CR full insert signal (RC&IS) 2. Reactor mode (PGCS)	1. CR control demand (RC&IS) 2. SB&PC pressure setpoint

Note: Various status signal interfaces are not shown in this table for brevity.

APR—Automatic Power Regulator

NMS—Neutron Monitoring System

PGCS—Power Generation Control System

RC&IS—Rod Control and Information System

SB&PC—Steam Bypass and Pressure Control System

TCS—Turbine Control System

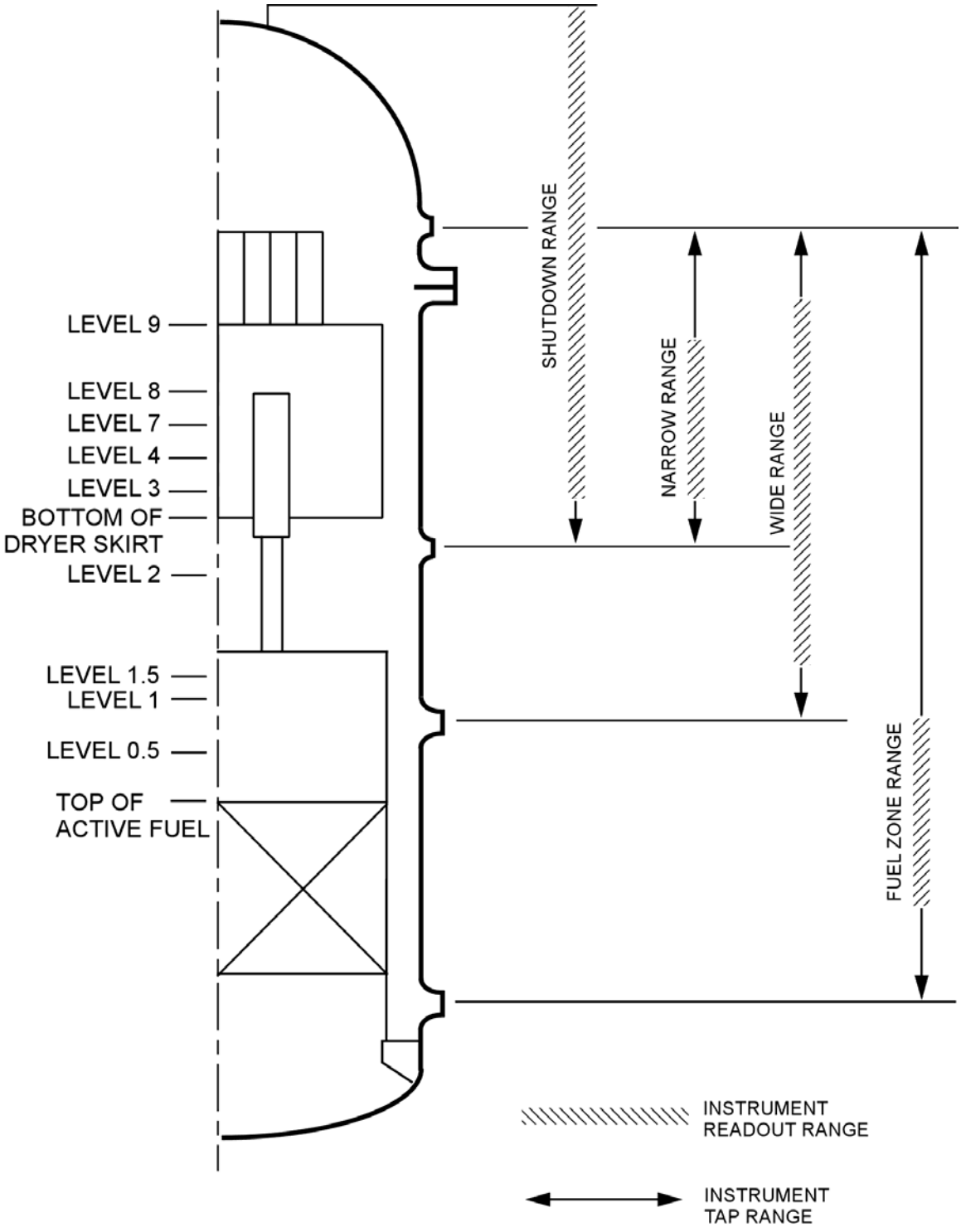
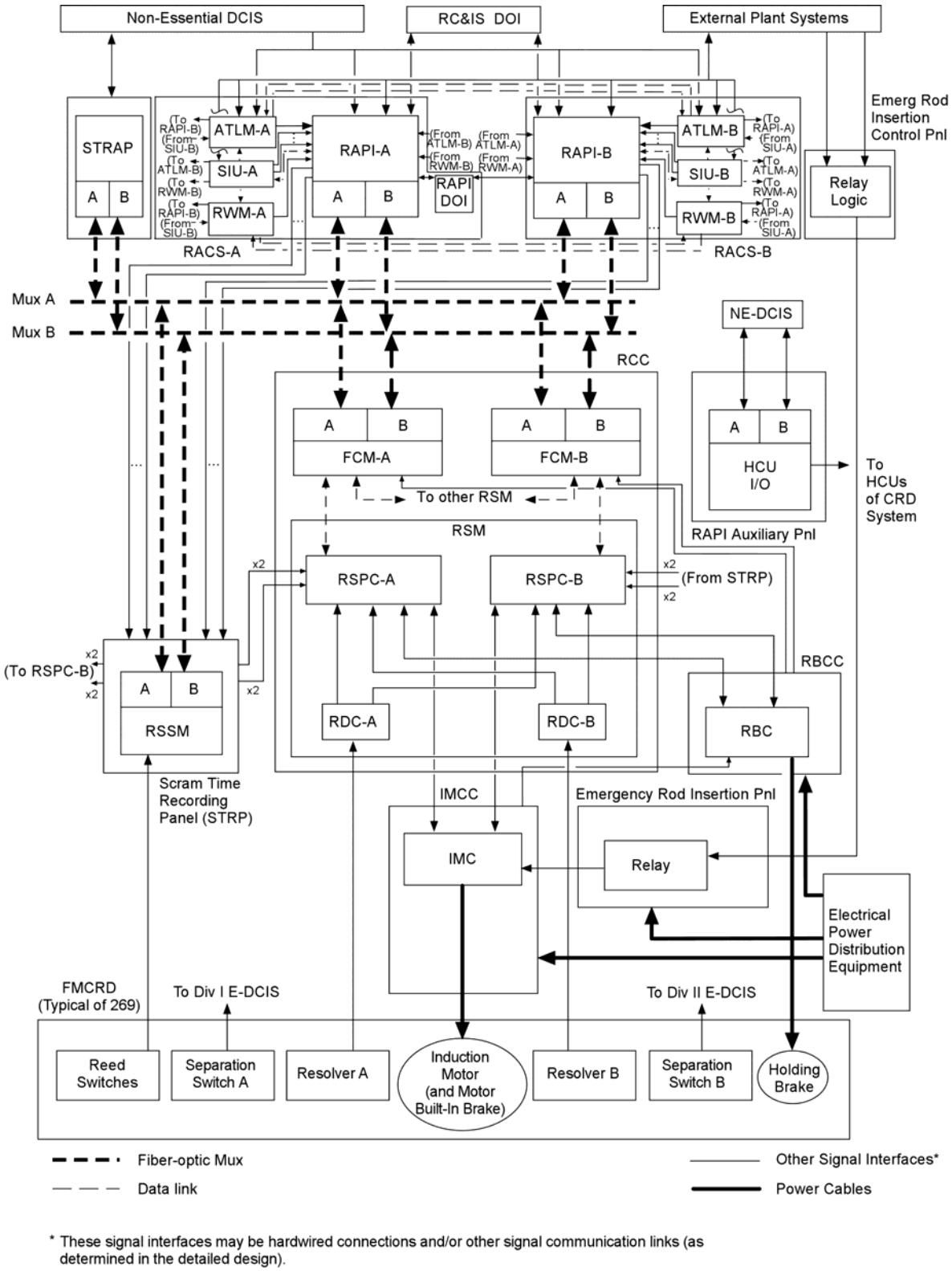


Figure 7.7-1. Water Level Range Definition



* These signal interfaces may be hardwired connections and/or other signal communication links (as determined in the detailed design).

Figure 7.7-2. RC&IS Block Diagram

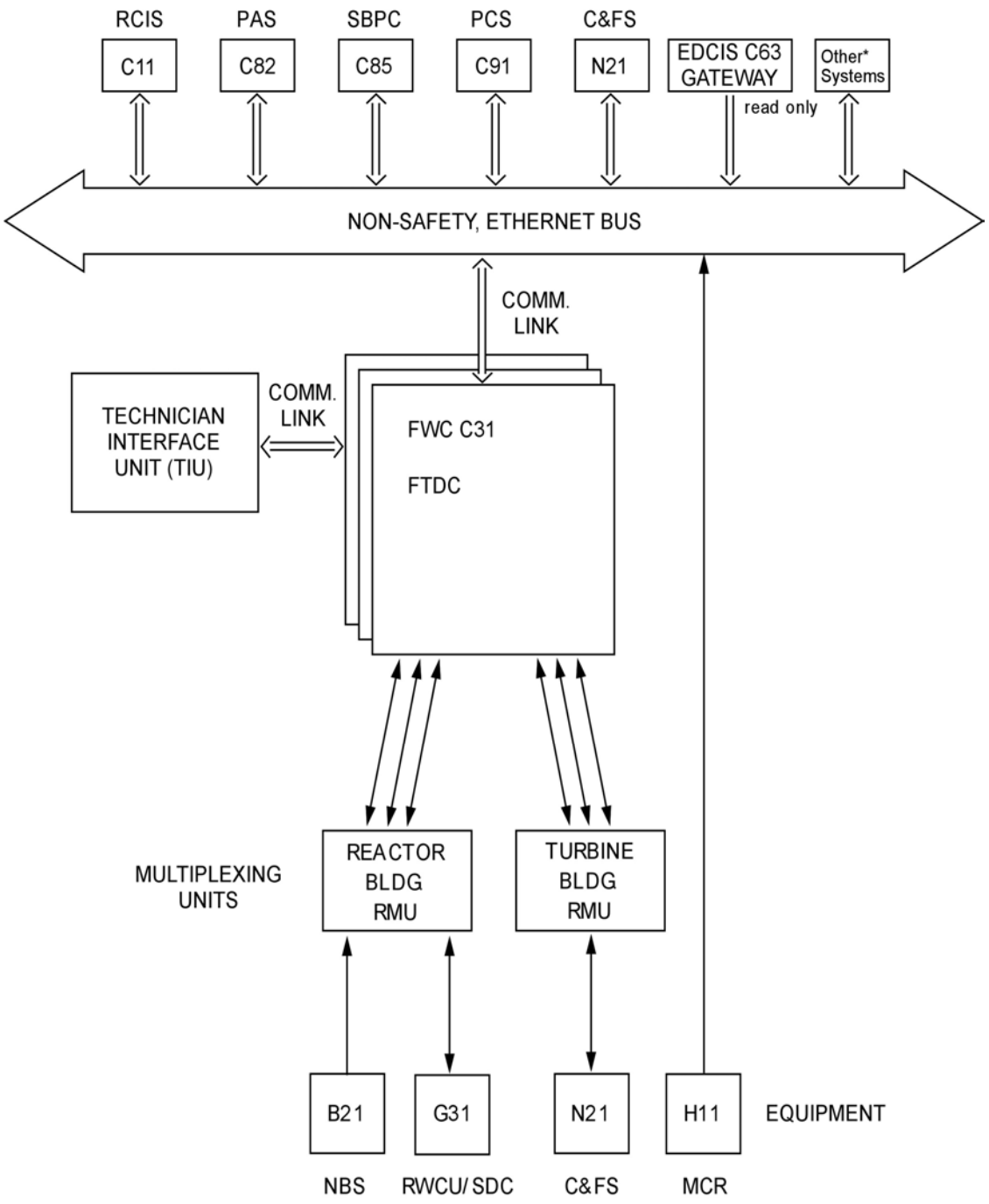


Figure 7.7-3. Feedwater Control System Functional Diagram

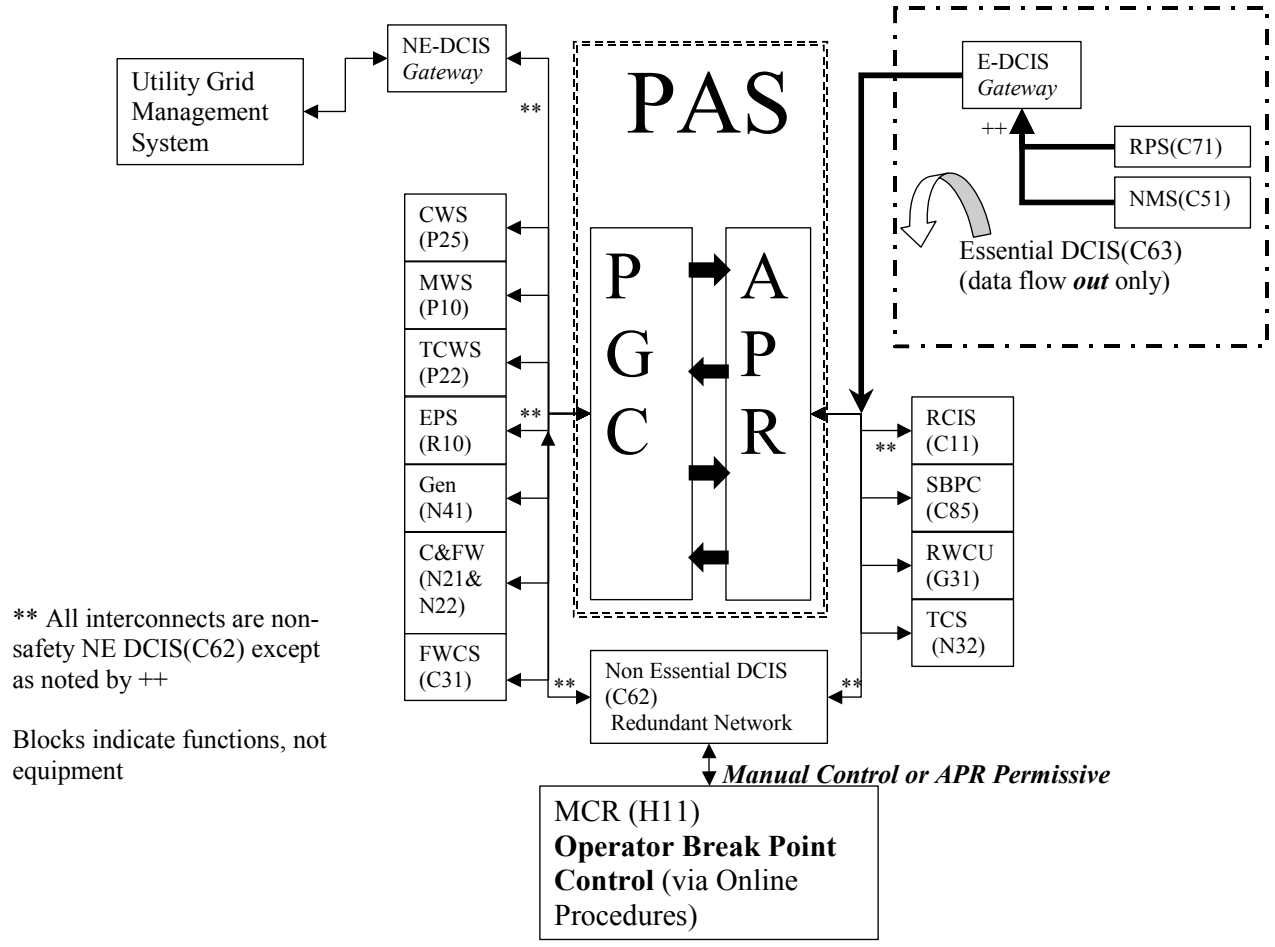


Figure 7.7-4. Plant Automation System Simplified Functional Diagram

(Only major systems are shown)

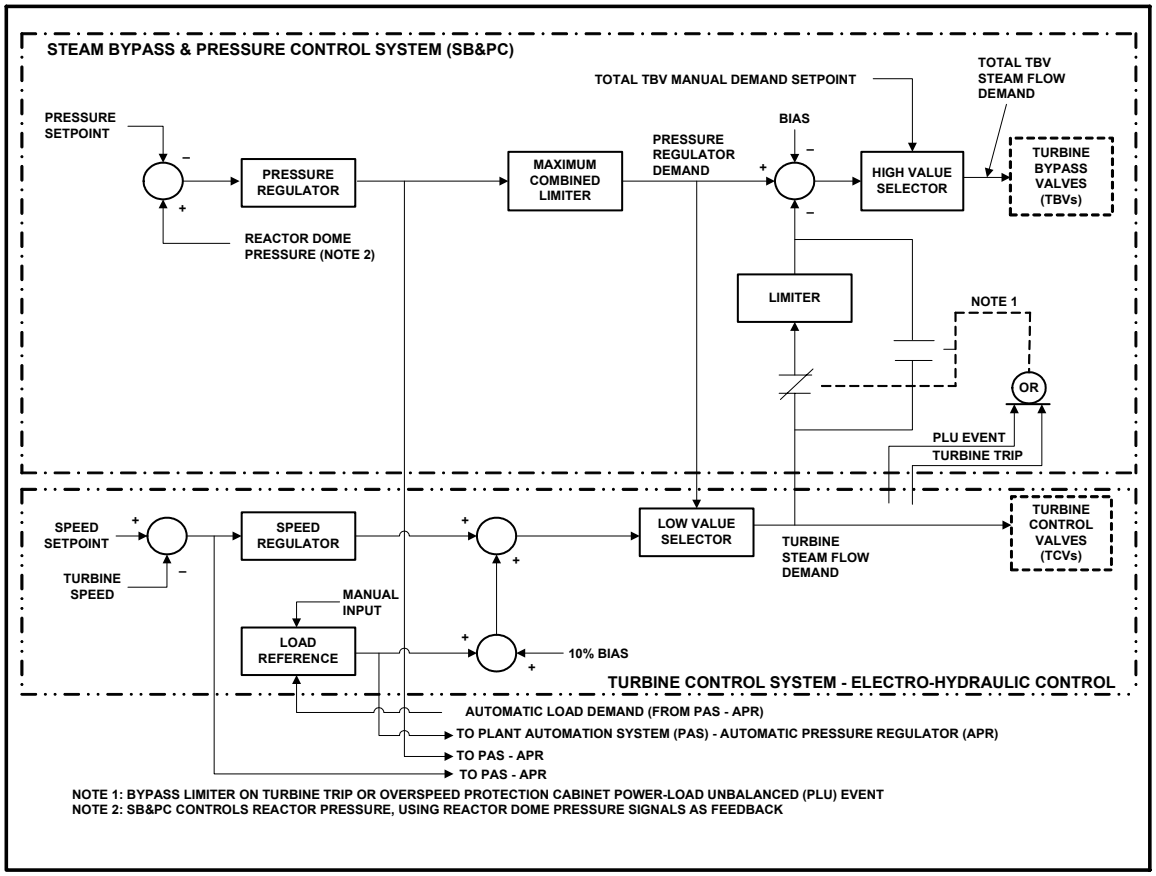


Figure 7.7-5. SB&PC Simplified Functional Block Diagram

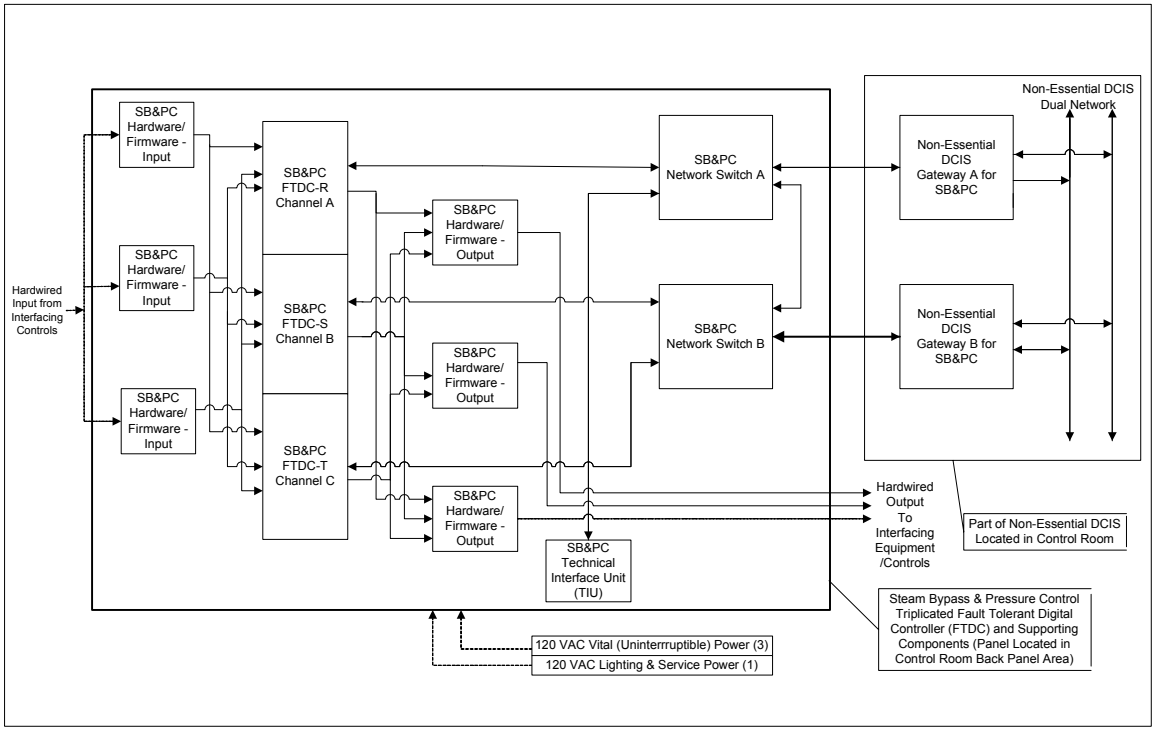


Figure 7.7-6. SB&PC FTDC Block Diagram

7.8 DIVERSE INSTRUMENTATION AND CONTROL SYSTEMS

7.8.1 System Description

Branch Technical Position (BTP) HICB-19 (1997) referenced in NUREG 0800 SRP Section 7 was developed in response to NRC concerns about common cause failures in software-based reactor protection system (RPS) and engineered safety features (ESF) systems (see References 7.8-1 and 7.8-2). This BTP requires a diverse instrumentation and control system be provided to ensure proper operation of RPS and ESF functions in the event of a common cause type failure of the primary protection systems. For the ESBWR, the diverse instrumentation and control system functions are provided by the Anticipated Transient Without Scram (ATWS) mitigation functions using the Standby Liquid Control (SLC) system and the Diverse Protection System (DPS). The ATWS mitigation functions and the DPS not only mitigate ATWS events but also ensure compliance with defense-in-depth requirements and protection against common mode failures as stated in the BTP–19. Mitigation of common mode failures, as described in the following subsections, is provided by the following diverse features including the DPS described in the following sections:

(1) Manual scram and Main Steam Isolation Valve (MSIV) isolation by the operator in the MCR in response to diverse parameter indications.

(2) Availability of diverse manual initiation of the passive ECCS functions including Gravity-Driven Cooling System (GDCS) squib valves initiation, Safety Relief Valve (SRV) initiation, and Depressurization Valve (DPV) initiation. Manual initiation functions are available both in the primary ECCS systems and in the DPS.

(3) Core makeup water capability from the feedwater, Control Rod Drive (CRD) System, and Reactor Water Cleanup (RWCU) System.

(4) Long-term shutdown capability provided in the Remote Shutdown System (RSS) with 2 divisional panels containing a manual scram control and safety and non safety related VDUs that allow control of all plant systems (if powered) and monitoring of all plant signals Local displays of process variables in RSS system are continuously powered and so are available for monitoring at any time.

(5) Diverse reactor protection (trip) initiation logic functions different from the primary RPS using separate and independent hardware with diverse software (part of the DPS)

(6) Diverse engineered safety features (ESF) initiation logic functions different from the primary ESF using separate and independent hardware with diverse software (part of the DPS.)

(7) ATWS mitigation using diverse means of liquid boron injection for emergency plant shutdown. This logic function resides in the Safety System Logic and Control (SSLC) as a safety-related four divisional logic function.

(8) ATWS mitigation using diverse means of alternate rod insertion (ARI) to hydraulically scram the plant using the three sets of air header dump valves of the control rod drive system. This logic function resides in the DPS together with the diverse RPS and diverse ESF functions. A simplified functional block diagram of the DPS is shown in Figure 7.8-1.

(9) Manual diverse initiation capability of the ATWS functions (ARI/SLC/Feedwater Runback).

The DPS is implemented as a nonsafety-related, triplicate redundant system, powered by nonsafety-related load group power sources.

With the primary SSLC, random failures are mitigated by the divisional sensor channel and output trip channel bypass capability of SSLC. A bypass places the remaining divisions in a 2-out-of-3 coincident logic condition such that another failure in a remaining division will not disable system operation.

7.8.1.1 ATWS Mitigation Functions

The Anticipated Transient Without Scram (ATWS) mitigation functions (Figures 7.8-2 through 7.8-4) use diverse control logics from the primary protection system:

(1) Automatic Standby Liquid Control (SLC) system initiation, as shown in Figure 7.8-3 and described in Subsection 7.4.1.

(2) Alternate Rod Insertion (ARI), as shown in Figure 7.8-2.

(3) Fine Motion Control Rod Drive (FMCRD) run-in (i.e., FMCRD Emergency Insertion), as shown in Figure 7.8-2, and also described Subsection 7.7.2, associated with the Rod Control and Information System (RC&IS).

(4) Feedwater Control System (FWCS) runback, as shown in Figure 7.8-3 and described in Subsection 7.7.3.

(5) Automatic Depressurization System (ADS) inhibit.

7.8.1.1.1 ATWS Mitigation Logic of SSLC

The safety-related portions of ATWS mitigation logic, which provide an alternate means of safe shutdown, are contained within the four divisions of SSLC, but as part of circuitry that is separate and diverse from the software-based RPS logic (Sections 7.2.1). Analog trip modules (ATMs), instead of Digital Trip Modules (DTMs), perform setpoint comparisons for the automatic trip parameters in each division. Hardware-based discrete digital logic substitutes for software-based trip logic to perform 2-out-of-4 voting logic. The hardware and software logic of this alternate emergency shutdown function is thus diverse from the hardware and software logic of the primary RPS function.

7.8.1.1.1.1 SSLC ATWS Logic Processors

There is a discrete-logic (non-microprocessor based) ATWS logic processor in each of the four SSLC cabinets (Figure 7.8-3). The ATWS logic processors are separate and diverse from RPS and other SSLC circuitry. These devices provide voting logic, control logic, and time delays for evaluating the plant conditions for automatic initiation of SLC boron injection and feedwater runback as part of the ATWS mitigation requirement:

(1) ATWS mitigation conditions and trips:

a. Automatic initiation of the SLC boron injection:

(i) High RPV dome pressure and a Startup Range Neutron Monitor (SRNM) ATWS permissive (i.e., SRNM signal above a specified setpoint) for 3 minutes or greater, or

(ii) Low reactor water level (L2) and a SRNM ATWS permissive for 3 minutes or greater.

(iii) LOCA start signal

b. Automatic initiation of feedwater runback:

High dome pressure and SRNM ATWS permissive for 2 minutes or greater. Reset permitted only when both signals drop below the setpoints.

(2) ATWS Logic Processor Functions:

a. Performs the 2-out-of-4 voting function and additional interlock logic on data from ATMs and Neutron Monitoring System (NMS).

b. Provides contact closure outputs hardwired to SLC and FWCS.

(3) ATWS Logic Processor Data Handling:

This device uses discrete gate logic (non-microprocessor based) and hardware timers to implement the ATWS mitigation logic. The input signals are hardwired (not multiplexed).

(4) ATWS Logic Processor Alarms:

a. INOP (instrument inoperative) to Non-Essential Distributed Control and Information System (NE-DCIS) (operating voltage degraded).

b. Division I (II, III, IV) ATWS SLC system injection logic tripped.

(i) Division I (II, III, IV) ATWS FWCS runback logic tripped.

Manual initiation of the ATWS SLC liquid boron injection is provided in the MCR (for manual SLC, ARI and Feedwater runback initiation).

The actuating signals for SLC system and FWCS are hardwired (not multiplexed) to their respective system controllers. If one of the four ATWS logic processors is inoperable, bypass signals are initiated to bypass the input signals from the out-of-service processor so that the input voting logic changes from 2-out-4 to 2-out-of-3. A manual bypass switch for this function is part of the SSLC Bypass Unit function in each division.

7.8.1.1.2 ATWS Mitigation Logic of Automatic Depressurization System (ADS) (part of Main Steam System)

For ATWS mitigation, ADS has an automatic and manual inhibit of the automatic ADS initiation. Automatic initiation of ADS is inhibited after there is a coincident low reactor water level signal and an average power range monitors (APRMs) ATWS permissive signal (i.e., APRM signal above a specified setpoint) from the NMS. There are main control room switches for the manual inhibit of automatic initiation of ADS. The same inhibit condition applies to GDCS function.

7.8.1.1.3 DPS ARI ATWS Mitigation Logic

Although the ARI function is part of the ATWS mitigation logic, it is nonsafety-related and is physically located in the DPS. The DPS has the logic to generate the following signals to mitigate an ATWS event (Figure 7.8-2):

(1) A signal to open the ARI valves (air header dump) in the CRD system on a high reactor vessel pressure signal, a low reactor water level signal, or a manual ATWS (ARI/SLC/FWRB initiation) signal.

(2) A signal to the RC&IS to initiate electrical insertion of all operable control rods on a high reactor vessel pressure signal, a low reactor water level (L2) signal, or a manual ATWS (ARI/SLC/FWRB initiation) signal.

This ARI/FMCRD Run-In logic resides in the DPS, which is totally separate and independent from the SSLC with both diverse hardware and software. The input sensors for the ARI logic are independent and separate from the sensors used in the SSLC system.

A manual ATWS (ARI/SLC/Feedwater runback initiation) signal initiates the SLC system, initiate the ARI, and initiates FWCS runback of feedwater flow.

7.8.1.2 Diverse Instrumentation and Control

In addition to the ATWS mitigation function that includes SLC function and diverse alternate emergency shutdown capabilities, other diverse instrumentation and control functions are included in the DPS. The DPS has a set of diverse protection and diverse engineered safety features (ESF) logics using separate and independent hardware and software from that of the SSLC. The DPS includes the diverse reactor protection functions, diverse ESF functions, and the ARI functions described in Subsection 7.8.1.1.3.

7.8.1.2.1 Diverse Reactor Protection Trip Functions

The DPS reactor protection trip functions are the diverse backup function to the primary RPS function to scram the reactor via control rod insertion. After evaluating the existing automatic scram initiation logics of the primary RPS, it is concluded that it is sufficient to include a subset of the existing RPS scram logic functions in the DPS to ensure acceptable diverse protection results. This set of diverse protection logics for reactor scram, combined with the ATWS mitigation features and other diverse backup scram protection and diverse ESF functions, provides the necessary diverse protections to meet the required design position called out in BTP HICB-19. The following scram signals are selected for inclusion in the DPS:

(1) High Reactor Pressure

(2) High Reactor Water Level (L8)

(3) Low Reactor Water Level (L3)

(4) High Drywell Pressure

(5) High Suppression Pool Temperature

This diverse set of RPS scram logics resides in independent and separate hardware and software equipment from the primary RPS. The process variables sensors that provide input to this diverse set of logics use different sets of sensors from that used in the primary RPS. The diverse

logic equipment is nonsafety-related with triplicate redundant channels. The power sources of this diverse equipment are from the nonsafety-related load groups. The scram initiation logic is "energize to actuate" with the trip signal actuators applied at the return side of the 120VAC circuit to the scram pilot valve solenoids, whereas the primary RPS scram initiation signal is applied at the supply side of the 120 VAC circuit. The trip logic is based on 2-out-of-3 voting.

7.8.1.2.2 Diverse Engineered Safety Features (ESF) Trip Functions

The ESBWR has several ESF functions including Gravity Driven Cooling System (GDCS) and automatic depressurization system function (ADS) using safety relief valves (SRV) and depressurization valves (DPV). It also has the pressure relief and core cooling function provided by the Isolation Condenser System (ICS). The ESF functions of GDCS, SRV and DPV are included in the DPS to provide diverse emergency core cooling system (ECCS) protections. The initiating logic is based on Level 1. This set of diverse protection logics for ESF function initiation, combined with the ATWS mitigation feature and other diverse backup scram protection and selected diverse RPS logics, provides the necessary diverse protections to meet the required design position called out in BTP HICB-19.

This set of diverse ESF logics resides in separate and independent hardware and software equipment from the primary ESF systems. The process variables sensors that provide inputs to this diverse set of logics use different sets of sensors from that used in the primary ESF systems. The diverse logic equipment is nonsafety-related with triplicate redundant channels. The diverse equipment power source is nonsafety-related. The initiation logic is "energize to actuate" similar to the primary ESF. The trip logic is based on 2-out-of-3 voting.

For the SRV opening function, two of the three SRV solenoids on each SRV are powered by two of the four divisional Class 1E power sources in the primary ESF ADS system. A third solenoid on each SRV is powered by the nonsafety-related load group, with the trip logic controlled by the DPS. All ten SRVs in the ADS are controlled by the DPS through the third solenoid on each valve.

For the DPV opening function, one of the two squib initiators on each DPV is controlled by and connected to the nonsafety-related DPS logic. However, the two squib initiators on each of all the DPVs are controlled simultaneously by the primary ESF ADS logic. The reliability and availability of DPV initiation by the primary ESF ADS function is not affected by the DPS logic. The typical initiation logic arrangements applied in both the ESF ADS and DPS functions are illustrated in Figure 7.3-1A and Figure 7.3-1B. As shown in Figure 7.3-1A and Figure 7.3-1B, the logic contacts circuit from the DPS is arranged in parallel with the ESF circuit. As described in Subsections 7.3.1.1 and 7.3.4, it takes two simultaneous SSLC/ESF trip signals to initiate the DPV squib valve opening. It also takes two simultaneous DPS trip signals in a dual redundant logic path to initiate the DPV squib valve opening. This satisfies the single failure criteria for inadvertent squib valve initiation. With this arrangement, the initiation of the DPVs by DPS logics does not affect the reliability and availability of the DPV initiation function controlled by the ESF logics.

The logic application to the GDCS squib valves from the SSLC/ESF and from the DPS is similar to that of the DPV logic application described above. The GDCS squib valves (short term injection) can be initiated both by the SSLC/ESF logic and by the DPS logic. For the GDCS squib valve opening function, one of the two squib initiators on each GDCS valve is controlled

by and connected to the nonsafety-related DPS logic. The logic has a dual redundant logic path for two simultaneous GDCS trip initiation signals to initiate a GDCS squib valve opening. Manual initiation capability is provided in the DPS logic circuitry to initiate the diverse ECCS functions of GDCS, SRV and DPV, respectively.

7.8.1.3 Diverse Manual Controls and Displays

All safety-related systems have displays and controls located in the main control room that provide for manual system-level actuation of their safety-related functions and monitoring of parameters that support those safety-related functions.

In addition to the manual controls and displays of the primary safety-related reactor protection and ESF functions, the DPS also has displays and manual control functions which are independent from those of the primary safety-related protection and ESF functions, and are not subject to the same common mode failure as the primary protection system components. The manual controls include the manual initiation of the SRV, GDCS valves, and the DPV, respectively.

The operator is provided with a set of diverse displays separate from those supplied through the safety-related, software-based logic. The displays listed below provide independent confirmation of the status of major process parameters:

- Reactor pressure
- Reactor pressure high alarm
- Reactor water level
- Reactor water level high alarm
- Reactor water level low alarm
- Drywell pressure
- Drywell pressure high alarm
- Suppression pool temperature
- Suppression pool temperature high alarm
- SRV solenoid-controlled valves opening
- DPV squib-initiation valves opening
- GDCS squib-initiation valves opening

In addition to the controls provided by the primary safety-related systems, the Remote Shutdown System (RSS) also provides manual control of shutdown cooling functions and continuous local display of monitored process parameters.

7.8.2 Common Mode Failure Defenses within Safety System Design

7.8.2.1 Design Techniques for Optimizing Safety-Related Hardware and Software

In addition to the inclusion of the DPS, techniques that are employed to ensure safety-related system reliability by minimizing both random and common mode failure probabilities are outlined below:

(1) The total amount hardware is minimized to assure highest reliability.

(2) Microprocessors with a simple operating system are used.

(3) The highest quality high precision components are used to gain reliability.

(4) To improve maintainability, self-diagnostics are implemented to locate any problem to a single assembly.

(5) The man-machine interface is implemented such that the equipment is structured into small units, with enough diagnostics so that a user can repair equipment by replacing modules and operate the equipment by following straightforward instructions.

(6) The software design process specifies modular code.

(7) Modules have one entry and one exit point and are written using a limited number of program constructs.

(8) Code is segmented by system and function:

a. Program code for each safety system resides in independent modules, which perform setpoint comparison, voting, and interlock logic.

b. Code for calibration, signal I/O, online-diagnostics, and graphical displays is common to all systems.

c. Fixed message formats are used for plant sensor data, equipment activation data and diagnostic data. Thus, corrupted messages are readily detected by error-detecting software in each digital instrument.

(9) Software design uses recognized defensive programming techniques, backed up by self-diagnostic software and hardware watchdog timers.

(10) Software for control programs is permanently embedded as firmware in controller Read only Memory (ROM).

(11) Commercial development tools and languages with a known history of successful applications in similar designs are used for software development.

(12) Automated software tools are used to aid in verification and validation (V&V).

Reliable software is implemented by ensuring that the quality of the design and requirements specification is controlled under the formal V&V program.

7.8.2.2 System Defense against Common Mode Failure

In addition to the DPS and the ATWS mitigation features, safety-related systems such as SSLC perform several simple, repetitive tasks continuously and simultaneously in four independent and redundant divisions of logic:

- setpoint comparison:
- 2-out-of-4 voting logic:
- control and interlock logic:
- Inputs and Outputs; and
- self-test.

The development of common software modules for many of these functions has the following advantages in producing reliable programs:

(1) Promotes standardization and code reusability;

(2) Minimizes program design errors;

(3) Minimizes timing differences among channels;

(4) Reduces software life cycle cost,

a. Simplifies V&V,

b. Reduces maintenance cost,

c. Simplifies future changes.

The V&V program reduces the probability of common mode failure to a very low level because the simple modules used in each division can be thoroughly tested during the validation process. In addition to software V&V, SSLC contains system level and functional level defenses against common mode failure, including defenses within the software itself, as follows:

(1) System level defenses against common mode failure

a. Operational defenses

(i) Asynchronous operation of multiple protection divisions; timing signals are not exchanged among divisions.

(ii) Automatic error checking on all multiplexed transmission paths. Only the last good data is used for logic processing unless a permanent fault is detected, thereby causing the channel to trip and alarm.

(iii) Daily (continuous by the plant computer) operator cross-check of redundant sensor inputs, in addition to automatic cross-checking.

(iv) Quarterly (continuous by the plant computer) surveillance of trip function (on-line with division bypass capability).

(v) Continuous self-test with alarm outputs in all system devices.

b. Functional defenses

(i) Instantaneous, simultaneous, and undetected failure on a common mode error is unlikely.

(ii) Automatic error detection permits early safe shutdown or bypass before common mode effects occur.

(iii) Separation and independence protect against global effects (EMI, thermal, etc.)

(2) Software defenses against common mode failure

The functional program logic in the SSLC controllers also provides protection against common mode failures, as follows:

a. Redundant sensors have data messages with unique identifications and time-tags in each division.

b. Modules that are identical are simple functions such as setpoint comparison and 2-out-of-4 voting that can be readily verified.

c. Multiplexing and other data transmission functions use standard protocols that are verified to industry standards and are also qualified to Class 1E standards.

7.8.3 Specific Regulatory Requirements Conformance

For diverse instrumentation and controls, Table 7.1-1 identifies the associated codes and standards applied in accordance with the Standard Review Plan. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the requirements conformance for each.

10 CFR 50.55a(a)(1), "Quality Standards."

The diverse instrumentation and controls are in conformance with this requirement.

10 CFR50.55a (h)

For the diverse instrumentation and controls, the applicable requirement is from ANSI/IEEE 279 item 4.7.2 (or IEEE 603 Item 5.6.3.1), 'Isolation Devices'. The transmission of signals between the equipment of protection systems (i.e., RPS and ESF systems) and control systems are performed via fiber optic links, which provide the required isolation.

10 CFR 50.62

The ATWS mitigation functions as described in Subsection 7.8.1.1 are designed in accordance with the requirements of 10 CFR 50.62, 'Requirements for reduction of risk from ATWS events for light-water-cooled nuclear power plants'.

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

52.47(a)(1)(vii) Interface Requirements

Conformance: Interface material is provided in Tier 1.

52.47(a)(2) Level of Detail

Conformance: The level of detail provided for this diverse I&C functions within the Tier 1 and Tier 2 documents conforms to this requirement.

52.79(c), ITAAC in Combined License Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with Table 7.1-1 and with the Standard Review Plan for Section 7.8 the following GDC are addressed for the diverse instrumentation and controls:

Criteria: GDC, 1, 13, 19, and 24.

Conformance: The diverse instrumentation and controls are in conformance with the GDC identified above.

The design of the diverse instrumentation and controls is such that RPS meets the requirements of 10 CFR 50 Appendix A, "General Design Criteria for Nuclear Power Plants," Section III, "Protection and Reactivity Control Systems."

Staff Requirements Memoranda (SRM)

Item II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087 (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs)

Conformance: The SRM requirements applicable to the diverse instrumentation and control functions state that " If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure as the safety system shall be required to perform either the same function as the safety system function that is vulnerable to common mode failure or a different function." It also states "The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary functions under the associated event conditions." With respect to manual control and display functions, it states "A set of displays and controls located in the main control room shall be provided for manual system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer systems." The implementation of the DPS and the ATWS mitigation features as described in Subsection 7.8.1, in conjunction with the RPS and ESF designs, conform with the above SRM requirements.

Regulatory Guides

In accordance with Table 7.1-1 and with the Standard Review Plan for Section 7.8 the following Regulatory Guides (RGs) are addressed as guidelines to Section 7.8, which includes the DPS and ATWS safety-related functions:

(1) RG 1.22 - Periodic Testing of Protection System Actuation Functions

(2) RG 1.62 - Manual Initiation of Protection Actions

(3) RG 1.75 - Physical Independence of electric systems

(4) RG 1.105 - Instrument Spans and Setpoints

(5) RG 1.118 - Periodic Testing of Electric Power and Protection Systems

(6) RG 1.152 - Digital Computers in Safety Systems of Nuclear Power Plants

(7) RG 1.153 - Power Instrumentation and Control Portions of Safety Systems

(8) RG 1.168 - Verification, Validation, Reviews and Audits for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(9) RG 1.169 - Configuration Management Plans for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(10) RG 1.170 - Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(11) RG 1.171 - Software Unit Testing for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(12) RG 1.172 - Software Requirements Specifications for Digital Computer Software used in Safety Systems of Nuclear Power Plants

(13) RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

Branch Technical Position (BTPs)

In accordance with Table 7.1-1 and with the Standard Review Plan for Section 7.8 the following BTPs are considered applicable and addressed as guidelines to Section 7.8, which includes the DPS and ATWS functions:

(1) BTP HICB-8 – Guidance on Application of Regulatory Guide 1.22

(2) BTP HICB-11 - Application and Qualification of Isolation Devices

(3) BTP HICB-12 - Establishing and Maintaining Instrument Setpoints

(4) BTP HICB-14 - Software Reviews for Digital Computer-Based Instrumentation and Control Systems

(5) BTP HICB-16 – Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

(6) BTP HICB-17 - Self-Test and Surveillance Test for Digital Computer-Based Instrumentation and Control Systems

(7) BTP HICB-18 - Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

(8) BTP HICB-19 - Evaluation of Defense in Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems

(9) BTP HICB-21 - Guidance on Digital System Real-Time Performance

7.8.4 COL Information

None

7.8.5 References

7.8-1 USNRC, "Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems," NUREG-0800, Appendix 7-A, Branch Technical Position HICB-19, June 1997.

7.8-2 USNRC, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,” Draft Regulatory Guide DG-1130 (Reg. Guide 1.152, Rev.2), December 2004.

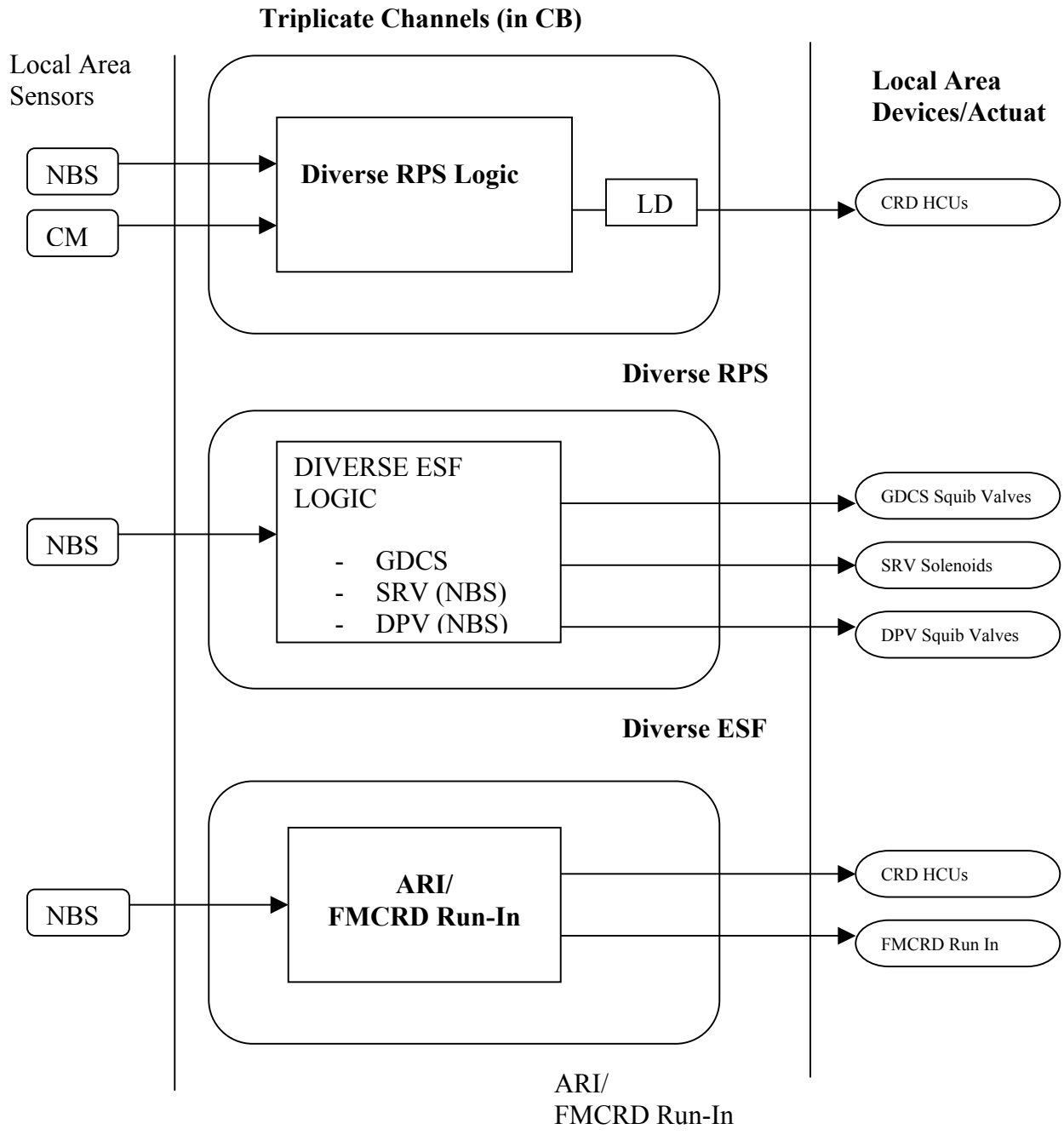
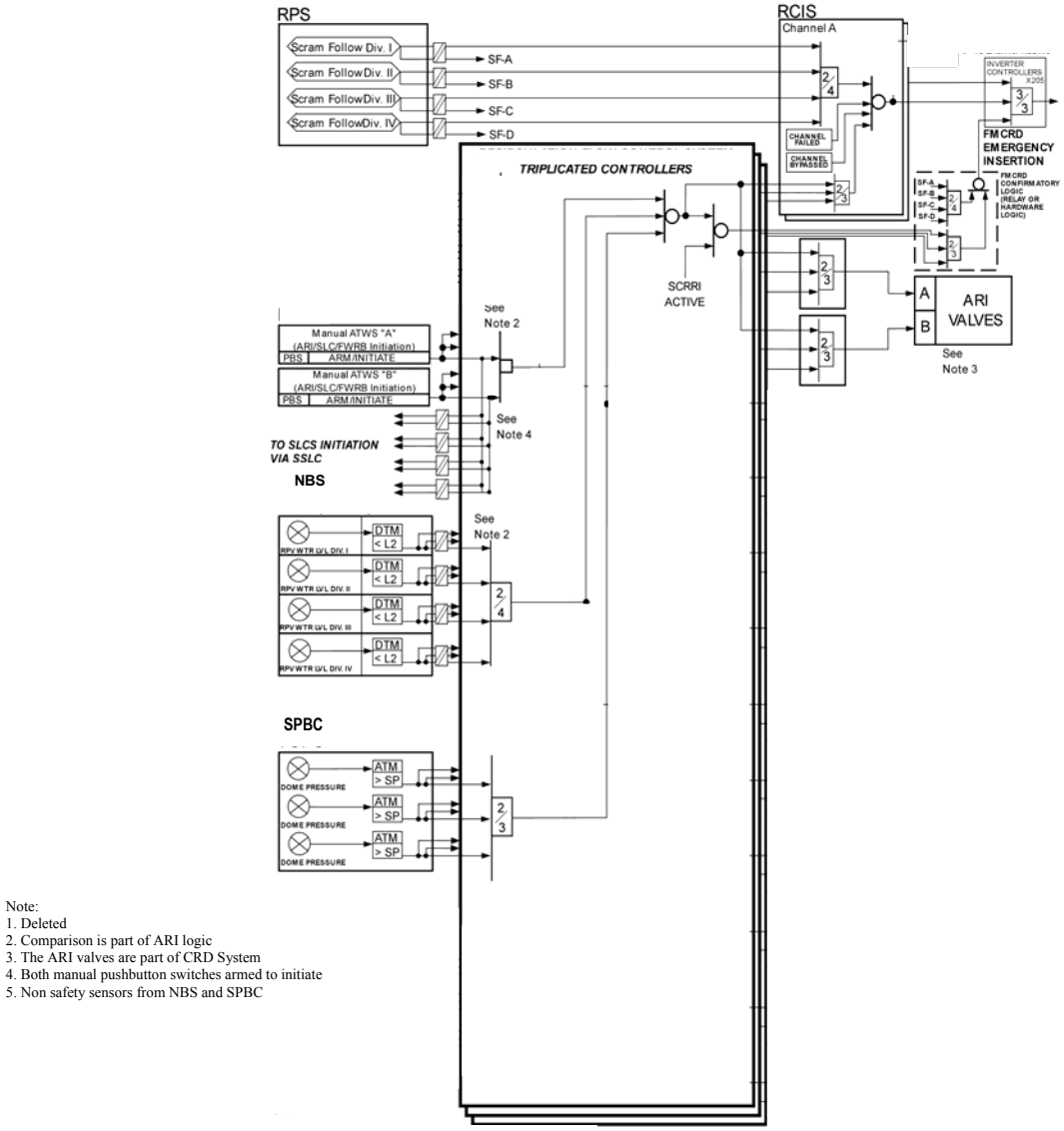
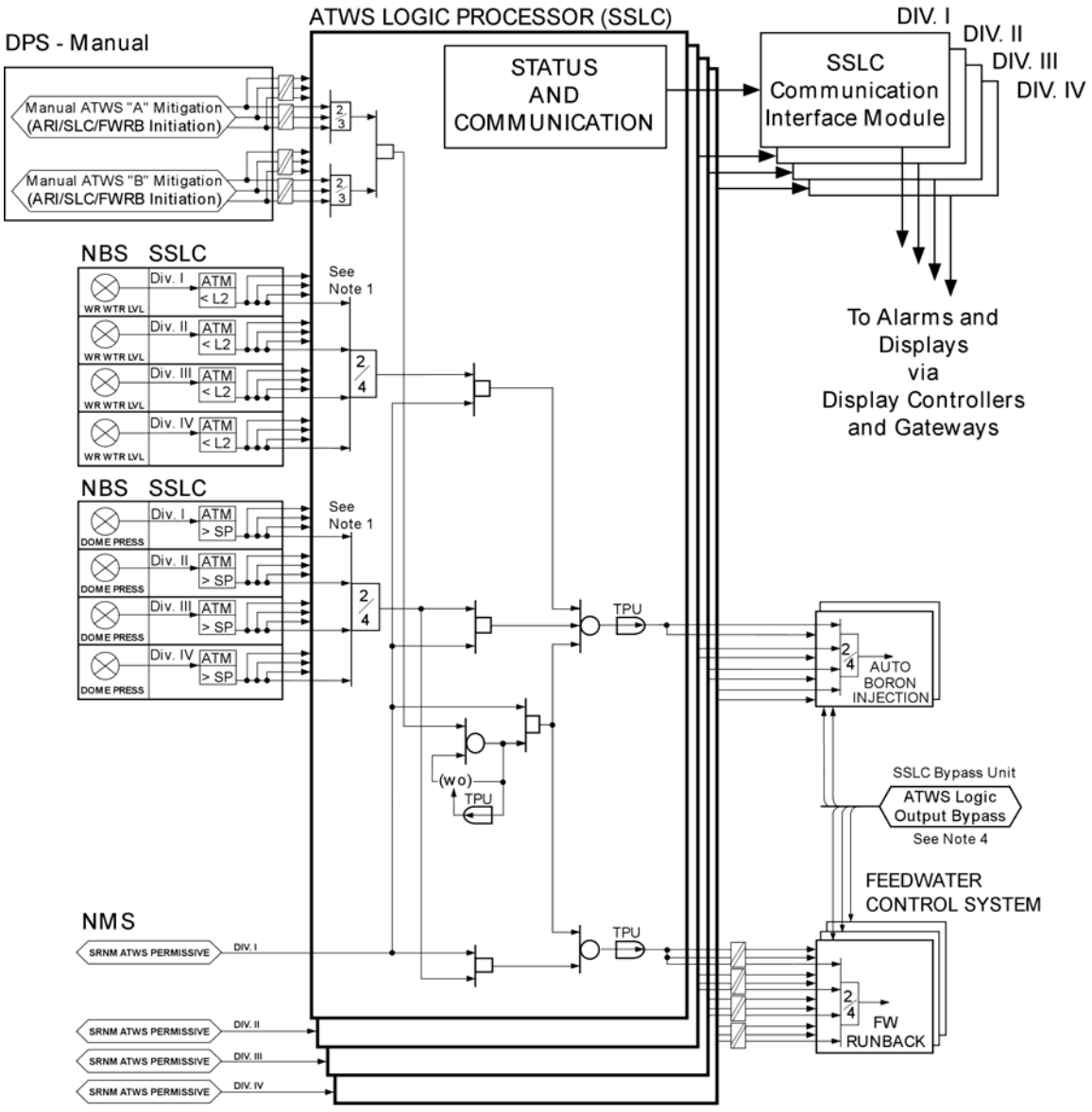


Figure 7.8-1. Simplified DPS Block Diagram



Note:
1. Deleted
2. Comparison is part of ARI logic
3. The ARI valves are part of CRD System
4. Both manual pushbutton switches armed to initiate
5. Non safety sensors from NBS and SPBC

Figure 7.8-2. ARI & FMCRD Run-In Logic



NOTES:

1. DIVISION-OF-SENSORS BYPASS INPUTS AND LOGIC NOT SHOWN.
2. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS EXCLUSIONARY LOGIC THAT RESULTS IN A "NO BYPASS" CONDITION FOR ALL DIVISIONS IF TWO OR MORE BYPASS INPUTS ARE RECEIVED.
3. THE ATWS LOGIC PROCESSOR SHALL INCLUDE DIVISION-OF-SENSORS BYPASS LOGIC THAT BYPASSES TRIP INPUTS FROM ALL SENSORS IN ONE DIVISION WHEN DIVISION-OF-SENSORS FOR THAT DIVISION IS PRESENT.
4. SEE SSLC LOGIC DIAGRAM FOR ATWS OUTPUT BYPASS LOGIC.
5. SLC FUNCTIONS IN ATM NOT SHOWN. SEE SLC LOGIC DIAGRAM.

Figure 7.8-3. ATWS Mitigation Logic (SLC system Initiation, Feedwater Runback)

7.9 DATA COMMUNICATION SYSTEMS

This section describes compliance with acceptance criteria for data communication systems that are part of or support the systems described in Sections 7.2 through 7.8.

The data communication system, or Distributed Control and Information System, consists of two parts, the safety-related Essential Distributed Control and Information System (E-DCIS), and the nonsafety-related Non Essential Distributed Control and Information System (NE-DCIS). This is described in the following sections.

7.9.1 Essential Distributed Control and Information System (E-DCIS)

7.9.1.1 Design Bases

Safety-Related Design Basis

The safety-related design bases of the E-DCIS are to:

- Read signals from the safety-related instrumentation via Remote Multiplexing Units (RMUs);
- Perform the required signal conditioning if this function is required; digitize and format the input signals into messages for transmission on the E-DCIS data network or data path;
- Transmit the data signals and commands onto the E-DCIS network or data path for interface with other safety related systems and main control room Video Display Units (VDUs); and
- Also transmit the actuation signals to safety-related equipment as output from the RMUs.

Power Generation Design Basis

The power generation design basis for the E-DCIS is to transmit plant parameters and other safety-related system data through isolation devices to the gateways that lead to the NE-DCIS that provide interfaces to nonsafety-related system logic and displays for power generation.

7.9.1.2 System Description

The E-DCIS provides communication interfaces and data process treatment to support the SSLC logic function and other safety-related systems for the safety-related systems and interface with the non-safety systems through the gateways to NE-DCIS. E-DCIS provides redundant and distributed instrumentation and control (I&C) data communications networks and data paths to support the monitoring and control of safety-related control and instrumentation systems from the input of safety related sensors to the RMUs, to the control signal output of the RMUs, to safety related system logic functions, actuation equipment and components. The E-DCIS system includes electrical devices and circuitry (such as remote multiplexing units, control processors, network switches, display devices, data communication paths and interfaces) that connect to field sensors, power supplies, and actuators, which are part of safety-related systems. The E-DCIS also includes any associated data acquisition and communications software, if required, to support its data distribution and control function.

E-DCIS replaces most of conventional, long-length, copper-conductor cables with a dual-redundant, fiber optic, data network. This reduces the cost and complexity of separated divisions

of cable runs that connect components of the plant protection and safety systems such as SSLC [Reactor Protection System, MSIV isolation logic functions, Leak Detection and Isolation System functions, Engineered Safety Features (ESF), etc.] and Class 1E Video Display Units. E-DCIS also provides an electrically noise-free transmission path for plant sensor data and safety system control signals.

SSLC and safety-related systems divisional data from sensors are received at safety-related remote multiplexing units (RMU), sensor signals conditioned if required, and then transferred to the divisional E-DCIS network to various video display units with soft controls, hard controls, workstations, and other SSLC and safety-related systems components connected to the network. In the E-DCIS, signals within divisional SSLC and safety-related systems instruments are transmitted to other safety-related systems via the network through dedicated interface connections.

There are divisionally separated redundant isolated digital gateways to provide one-way communications from divisional E-DCIS networks to the NE-DCIS. The communication from nonsafety-related systems to the E-DCIS is limited to communication from the 3D Monicore function of the NE-DCIS to the PRNM function of the Neutron Monitoring System (NMS). (Refer to Subsection 7.2.2.4.2.) This data communication is a dedicated input to NMS and does not pass through the E-DCIS network.

The interconnections among Division I, II, III and IV of E-DCIS are provided by isolated digital interfaces while physical and electrical isolation between divisions are maintained. The isolated digital interface functions, i.e., the communication interface modules of the safety SSLC system, provide communications between divisions.

For the E-DCIS data communication, the system timing for each division is asynchronous with respect to other divisions, i.e., there is no common system clock and no timing data is exchanged. Acquired data is time tagged at the safety to non-safety gateways with a common time of day for convenience in logging and recording, but the time tag is not required or used for safety-related functions.

The local E-DCIS RMU performs signal conditioning and A/D signal conversion for continuous process signals, and performs signal conditioning and change-of-state detection for discrete signals such as contact closures/openings. The RMU function can be applied for performing both input and output signal processing functions. The RMU formats the acquired signals into data messages and transmits the data via the dual redundant data path network to the various SSLC and safety-related systems components for logic processing. The RMU designated as logic output processor then receives such trip command and control signals from SSLC and safety-related system components via the network. It then provides terminal points for distributing the signals to the final actuating devices of the safety systems.

The supervision of SSLC logic modules data reception and transmission is handled by the SSLC network interface module (NIM). The NIM is connected to the network. Operator interfaces for control and display is realized through the visual display unit (VDU), which is also connected to the network. An illustration of a typical division of E-DCIS that includes network and data paths interfacing with the associated SSLC and safety-related system components (e.g., RPS and NMS) are shown in Figure 7.9-1.

E-DCIS contains continuous online-diagnostic functions that monitor transmission path quality and integrity. The dual redundant data communication channels are repairable on-line if one channel fails. E-DCIS failures are alarmed in the MCR. The dual redundant data communication channels per division and the four redundant divisions of the E-DCIS satisfies the single failure criterion of the IEEE Std. 603. It also satisfies the independence, testing, and repair requirements as outlined in IEEE Std. 603. The fiber optic cable and network that are part of the E-DCIS under four redundant divisions satisfy the separation and independent requirements of division equipment including cable routing separation, which meets the requirements as required by NUREG-0800 Standard Review Plan (SRP) 9.5.1, Fire Protection Programs. Periodic surveillance, using off-line tests with simulated input signals, is used to verify the overall system integrity. Segments of E-DCIS can be tested (and calibrated if needed) on-line when portions of SSLC are bypassed. Any E-DCIS control equipment software, such as that in the RMU, is implemented based on read only memory that cannot be modified by plant personnel. E-DCIS power is supplied by the divisional 120 VAC safety-related power supply systems.

7.9.1.3 Safety Evaluation

The E-DCIS forms an integral part of the safety-related systems and SSLC protection function and parallels the four-division design of that system. No failure of a single division can prevent a safety-related action (detection, trip, etc.) from being accomplished successfully. Component self-test reconfigures the system to the approved safe state upon detection of uncorrectable errors. Off-line test and calibration of E-DCIS components is designed into the system. Individual divisions may be disconnected for maintenance and calibration through bypass within the SSLC division without compromising the other divisions' operations.

Specific Regulatory Requirements Conformance

Table 7.1-1 identifies the E-DCIS and the associated codes and standards applied in accordance with the Standard Review Plan (SRP). The following analysis lists the applicable criteria and discusses the conformance for each.

10 CFR 50.55a (IEEE 279)

Conformance: Addressing RG 1.153 and IEEE 603 satisfy 10 CFR 50.55a.

10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety"

Conformance: The E-DCIS conforms to this requirement.

10CFR 50.55a(h), "Protection Systems," which requires compliance with ANSI/IEEE Std 279, and ANSI/IEEE Std 279, item 4.7.2, "Isolation Devices"

Conformance: The E-DCIS conforms to this requirement. Refer to Subsections 7.2.1.3, 7.1.2.3.3 and 7.1.2.3.6 for additional discussion.

10 CFR 50.34(f)(2)(v), "Automatic Indication of Bypassed and Inoperable Status of Safety System Equipment."

Conformance: The E-DCIS conforms to this requirement. Refer to Subsection 7.2.1.3 for additional discussion.

10 CFR 50.62, "Requirements for the Reduction of Risk from Anticipated Transients without Scram."

Conformance: The E-DCIS conforms to this requirement, in conjunction with the ATWS mitigation functions as described in Subsection 7.8.1 and 7.8.3.

10 CFR 52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Conformance: Resolution of unresolved and generic safety issues is discussed in Section 1.11.

10 CFR 52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

10 CFR 52.47(a)(1)(vii) Interface Requirements

Conformance: Interface material is provided in Tier 1.

10 CFR 52.47(a)(2) Level of Detail

Conformance: The level of detail provided for the RPS within the Tier 1 and Tier 2 documents conforms to this requirement.

10 CFR 52.47(b)(2)(i) Innovative Means of Accomplishing Safety Functions

Conformance: The ESBWR is designed with innovative means of accomplishing safety functions, as delineated in Section 1.5.

10 CFR 52.79(c), ITAAC in Combined License Applications

Conformance: ITAAC are provided for the I&C systems and equipment in Tier 1.

General Design Criteria (GDC)

In accordance with the SRP for Section 7.9 and Table 7.1-1, the following GDC are addressed for the E-DCIS:

- Criteria: GDC 2, 4, 13, 19, 21, 22, 23, 24, and 29.
- Conformance: The E-DCIS is in compliance with these GDC.

Staff Requirements Memoranda:

- **Item II.Q (Defense Against Common-Mode Failures in Digital Instrument and Control Systems) of SECY-93-087** (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs)
- Conformance: The E-DCIS conforms to the Item II.Q of SECY-93-087 (BTP HICB-19) in conjunction with the implementation of diverse instrumentation and controls, described in Section 7.8.
- **Item II.T [Control Room Annunciator (Alarm) Reliability] of SECY-93-087** (Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs) – Refer to Subsection 7.1.2.2 and Section 7.5 for compliance discussion.

Regulatory Guides (RGs)

In accordance with the SRP for Section 7.9 and Table 7.1-1, the following RGs are addressed for the E-DCIS:

RG 1.22 - Periodic Testing of Protection System Actuation Functions – The E-DCIS fully supports compliance with the guidance of RG 1.22. The E-DCIS is a communications system supporting SSLC and safety-related system operation. The E-DCIS is designed to fully support SSLC testing and device actuation by providing the same divisional redundancy and separation as the system it supports. Periodic testing of the SSLC and other safety-related systems also test the E-DCIS.

RG 1.47 - Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems – SSLC provides bypass capability and status indication that are displayed on the E-DCIS video display units VDU(s). The E-DCIS provides network inoperable status indications that a network fails to communicate properly.

RG 1.53 - Application of the Single-Failure Criterion to Nuclear Power Protection Systems – The E-DCIS meets the requirements of RG 1.53 in addition to Section 5.1 of IEEE 603 and IEEE 379.

RG 1.75 - Physical Independence of Electric Systems – The E-DCIS fully complies with the guidance of RG 1.75 and the requirements of IEEE 384.

RG 1.105 – Instrument Setpoints for Safety Systems – E-DCIS does not include the sensors and actuators, which are input/output from the RMUs. E-DCIS and SSLC conform to the requirements of RG 1.105.

RG 1.118 - Periodic Testing of Electric Power and Protection Systems – The E-DCIS conforms to the intent of RG 1.118 as amplified in IEEE 338. Testing of the E-DCIS is done in conjunction with the SSLC.

RG 1.152 - Criteria for Digital Computers in Safety Systems of Nuclear Power Plants - The E-DCIS fully complies with this regulatory guide. The hardware and software within E-DCIS in conjunction with SSLC for the RPS function and other safety systems are developed in compliance with this Reg. Guide, which endorses IEEE Std. 7-4.3.2.

RG 1.153 - Criteria for Power, Instrumentation, and Control Portions of Safety Systems – The E-DCIS in conjunction with the SSLC fully conforms to this regulatory guide.

RG 1.168 - Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.169 - Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.170 - Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.171 - Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.172 - Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

RG 1.173 - Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants - Refer to Subsection 7.1.2.2 for compliance discussion.

Branch Technical Positions (BTPs)

In accordance with the SRP for Section 7.9 and Table 7.1-1, the following BTPs are addressed for the E-DCIS:

BTP HICB-8 - Guidance on Application of Regulatory Guide 1.22 – The E-DCIS is fully operational during reactor operation and is tested in conjunction with the SSLC. Therefore, the E-DCIS fully meets this BTP.

BTP HICB-11: Guidance on Application and Qualification of Isolation Devices— Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

BTP HICB-12: Guidance on Establishing and Maintaining Instrument Setpoints - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to the guidance of this BTP.

BTP HICB-16: Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52 - This BTP is applicable to all section of the DCD including this section on E-DCIS.

BTP HICB-17: Guidance on Self-Test and Surveillance Test Provisions in Digital Computer-based Instrumentation and Control Systems. - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

BTP HICB-18: Guidance on Use of Programmable Logic Controllers in Digital Computer-based Instrumentation and Control Systems - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

BTP HICB-19: Guidance for Evaluation of Defense-in-Depth and Diversity in Digital Computer-Based Instrumentation and Control Systems (Item II.Q of SECY-93-087) - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

BTP HICB-21: Guidance on Evaluation of Digital System Architecture and Real-Time Performance - Refer to Subsection 7.2.1.3 discussion. The E-DCIS conforms to this BTP.

7.9.1.4 Testing and Inspection Requirements

All components of E-DCIS are readily accessible for testing purposes. The continuous automatic online-diagnostics of E-DCIS detect most data transmission errors and hardware failures at the card level. Continuous self-diagnostics in each RMU monitors the status of each module. A comprehensive, off-line, network performance test is conducted regularly to confirm that the data transmission capability is functional as intended. This test confirms that data error rates are within specified limits, signal quality is within specifications, and the network is capable of handling the required throughput.

Because the E-DCIS functions are closely interfaced with the SSLC functions, the integrated hardware and software functions of the E-DCIS and SSLC including network parameters and data status are checked and tested. Some of the key diagnostics include the CPU status check, parity checks, watchdog timer status, voltage level in controllers, data path integrity and data validation checks, and data cycling time and system signal response time. The analog-to-digital (A/D) converters (also the digital-to analog converters if used) in the RMUs are the only components requiring periodic calibration checks. Calibration can be performed automatically. In E-DCIS, online-diagnostics are qualified as safety-related in conjunction with functional software qualification.

A detected hardware failure results in an alarm in the MCR. Corrupted data are detected through error detection functions in the network.

7.9.1.5 Instrumentation and Control Requirements

E-DCIS does not include sensor inputs up to the RMUs and RMU outputs to actuators. The data transmission function provides for the delivery of system data to all nodes in the network (i.e., to distributed logics of the E-DCIS RMUs and certain SSLC system components), and in certain safety-related systems through dedicated data paths. The E-DCIS thus provides the necessary integrated support for the distributed control logic functions of the RMUs and SSLC equipment. The data I/O and transmission functions do not require any manual operator intervention and have no operator controls.

The E-DCIS operates continuously in all modes of plant operation to support the data transmission requirements of the various interfacing systems. When a network of the dual network system fails, operation continues automatically without operator intervention. In the event that a channel failure occurs, the network alarms in the main control room, indicating the failed component. The failed segment of the channel can be isolated from the operating segments and can be repaired on-line.

The following E-DCIS displays and alarms, as a minimum, are provided in the main control room:

- MCR Alarms
  - E-DCIS Division I Trouble
  - E-DCIS Division II Trouble
  - E-DCIS Division III Trouble
  - E-DCIS Division IV Trouble
- MCR Indications
  - E-DCIS Division I diagnostic displays
  - E-DCIS Division II diagnostic displays
  - E-DCIS Division III diagnostic displays
  - E-DCIS Division IV diagnostic displays.

7.9.2 Non-Essential - Distributed Control and Information System (NE-DCIS)

7.9.2.1 Design Bases

Safety (10 CFR 50.2) Design Basis

The NE-DCIS system does not perform or ensure any safety-related function. It is classified as a nonsafety-related system, and has no safety-related design basis.

Power Generation (Non-safety) Design Bases

The NE-DCIS system is required to:

- Provide a communication path for nonsafety-related data gathered and distributed throughout the various areas of the plant, including datalink interfaces to control systems and data communication networks provided with the Turbine Control System, Feedwater Control System, Steam Bypass & Pressure Control System, Plant Automation System – Automatic Power Regulator, the Triple Modular Redundant (TMR) systems and other systems such as condensate polishing, offgas, radwaste, and meteorological;
- Reliably transfer to or from the plant areas, in digital format, analog or binary information, that has been collected and digitized from nonsafety-related Remote Multiplexing Units (RMUs); these include transmitters, contact closures and other sensors or process activation signals, generated elsewhere, for the control of remote devices such as pumps, valves or solenoids;
- Receive selected safety-related signals from Essential - Distributed Control and Information System (E-DCIS) through gateway devices, or workstations, then transmit to non safety-related video display units and non safety-related systems for control purposes;
- Replace a majority of conventional, long-length, copper-conductor cables that connect components of the nonsafety-related plant instrumentation systems and control systems with fiber optic data networks to reduce cost and complexity of cable runs;
- Provide an electrically noise-free transmission path for plant sensor data and control signals;
- Collect and archive data for transient analysis and data archiving, sequence of events recording, display of Safety Parameter Display information in the main control room, processing, and annunciation of alarm conditions to plant operational staff;
- Perform the Plant Computer Functions (PCF) – Performance Monitoring and Control (PMC) by providing nuclear steam supply (NSS) performance and prediction calculations, video display control, point log and alarm processing and balance-of-plant (BOP) performance calculations.

  PCF increases the efficiency of plant performance by:

  – performing the functions and calculations defined as being necessary for the effective evaluation of nuclear power plant operation;

- providing the capability for supervisory control of the entire plant by supplying setpoint commands to independent nonsafety-related automatic control systems as changing load demands and plant conditions dictate;
- providing a permanent record and historical perspective for plant operating activities and abnormal events;
- providing analysis, evaluation and recommendation capabilities for startup, normal operation, and plant shutdown;
- providing capability to monitor plant performance through presentation of video displays in the MCR and elsewhere throughout the plant; providing the ability to directly control certain nonsafety-related plant equipment through on-screen technology;
- providing an interface to the plant simulator for training and for development and analysis of operational techniques; and
- facilitate communication and exchange with the Technical Support Center (TSC) and the Emergency Operation Facility (EOF).

The calculations performed by PCF include process validation and conversion, combination of points, nuclear system supply performance calculations, and balance-of-plant performance calculations.

The PMC provides nuclear steam supply (NSS) performance and prediction calculations, video display control, point log and alarm processing and balance of plant (BOP) performance calculations.

NSS Performance Module - The NSS performance module provides the reactor core performance information. The calculations performed are as follows:

(1) The local power density for every fuel assembly is calculated using plant inputs of pressure, temperature, flow, LPRM levels, control rod positions, and the calculated fuel exposure.

(2) Total core thermal power is calculated from a reactor heat balance. Iterative computational methods are used to establish a compatible relationship between the core coolant flow and core power distribution. The results are subsequently interpreted as power in specified axial segments for each fuel bundle in the core.

(3) The core power distribution calculation sequence is completed periodically and on demand. Subsequent to executing the program, the computer prints a periodic log for record purposes. Key operating parameters are evaluated based on power distribution and edited on the log.

(4) Flux level and position data from the automatic fixed in-core probe (AFIP) equipment are read into the computer. The computer evaluates the data and determines gain adjustment factors by which the LPRM amplifier gains can be altered to compensate for exposure-induced sensitivity loss. The LPRM amplifier gains are not to be altered except immediately prior to calibration using the AFIP system. The gain adjustment factor

computations help to indicate to the operator when such a calibration procedure is necessary.

(5) Using the power distribution data, a distribution of fuel exposure increments from the time of the previous power distribution calculation is determined and is used to update the distribution of cumulative fuel exposure. Each fuel bundle is identified by batch and location, and its exposure is stored for each of the axial segments used in the power distribution calculation. These data are printed out on operator demand. Data necessary in determining the lifetime of a control rod is calculated based on the integrated affect of control rod positions and power distributions and is printed on operator demand.

(6) The exposure increment of each local power range monitor is determined periodically and is used to update both the cumulative ion chamber exposures and the correction factor for exposure-dependent LPRM sensitivity loss. These data are printed out on operator demand.

In addition, the following functions are performed under the architecture of NE-DCIS:

- ***Safety Parameter Displays***. The Safety Parameter Displays provide critical plant operating parameters such as power, water level, temperatures, pressure, flows, and status of pumps, valves, etc., for main control room operators to follow the plant emergency operating procedures (EOPs) to shutdown the reactor, maintain adequate core cooling, cool down the reactor to cold shutdown conditions and maintain primary containment integrity as required by the NUREG-0737, Supplement 1.

- ***Main Control Room (MCR) Displays.*** The Main control room panel equipment is part of the Main Control Room Panels System. See Section 18.4 for detailed description. Information for the displays is presented with the following functional configuration arrangement:

  The plant computer function MCR displays are functionally classified as follows:

  – Level – 0: Integrated overview display

  – Level – 1: Navigational/top level display

  – Level – 2: System level display

  Integrated Overview Display

  – The Large Display (wide display) Panel of the plant computer functions provides the plant integrated overview display.

  – The fixed-position portion of the large display panel provides the critical plant operating information such as power, water level, temperature, pressure, flow and status of major equipment and availability of safety systems with mimic in the main control room during plant normal, abnormal and emergency operating condition. (The dynamic display elements of the fixed-position displays are driven by dedicated microprocessor-based controllers, which are independent of the NE-DCIS. Certain safety-related information is not from NE-DCIS.

– The large variable portion of the panel display provides the display(s) of any plant computer function (PCF) (driven by NE-DCIS VDUs) screen format available on the main control console video display units.

Navigational or Top Level Displays - The plant computer function will provide the following navigational or top level displays:

– Safety Parameter Displays

– Alarms and Annunciators

– Power Generation Control

– On-line Procedures

– Tech Spec Monitor/Reactor Protection System Monitor

– 3D MONICORE

Historian

Transient Recording and Analysis

– Thermal Performance Monitor and Diagnostic

– Report Generator

– Bypass and Inoperable Status Indication (BISI)

System Level Display

– The PCF control displays provide direct control and parameter monitoring of nonsafety related equipment and systems through the use of electronic touch screens, CRTs and various input devices**,** which are part of the Main Control Room Panels.

– The RC&IS Dedicated Operator Interface provides for control and monitoring of the RC&IS. This interface is not part of the PCF scope (*The RC&IS interface is described in Subsection 7.7.2.2).*

- ***Alarms & Annunciation:*** at the MCR Video Display Units (VDUs), Technical Support Center (TSC), Emergency Operations Facility (EOF)

  The plant Alarm and Annunciators subsystem (AAS) is designed to:

  – Alert the operators to off-normal conditions which require them to take action;

  – Guide the operators, to the extent possible, to the appropriate response;

  – Assist the operators in determining and maintaining an awareness of the state of the plant and its systems or functions;

  – Minimize distraction and unnecessary workload placed on the operators by the alarm system.

  – The AAS is designed to satisfy the dark panel concept: no alarm signal shall be shown to the operator when the process is operating normally without malfunctioning at power.

- Function and task analysis are be used to determine system level alarms.
- The alarm display function includes means of providing the operator the
- information in different views including sorting, filtering, and grouping of alarms.
- The alarm generation function generates different types of alarms, both basic alarms and high-level (composite) alarms. All the generated alarms are subject to potential filtering, alarm suppression, and alarm prioritization. Alarms are then presented in the control room through fixed-position alarm tiles on the large display panel.
- There will be the capability for operators to create temporary user definable alarms and associated alarm setpoints.

- ***On Line Procedures (OLP)***

  OLP provides for:

  - Display of normal, abnormal and emergency operating procedures on operator
  - workstations and workstations where display of operating procedures is permitted.
  - Display of operating procedures in logic (flowchart) and text formats.
  - Display of operating procedures.
  - Hardcopy output of operating procedures from all workstation locations with the same format and content as displayed, considering potential uses as alternatives for study guides, procedure maintenance, etc.
  - Maintenance (addition, deletion, modification) of operating procedures.
  - Manual, semi-automated (selected procedures), or fully automated (selected procedures) performance of operating procedures from the operator workstations.
  - Access to controls from the displayed operating procedures.
  - Continuously updated display of parameters, to include embedded dynamic indication status (normal, warning, alarm conditions), necessary for the plant operator to monitor and/or perform operating procedure steps.
  - Confirmation of operator decisions and actions while retaining the operator as the final authority in the execution of procedures.
  - Logging all discrepancies between the operator's decisions and actions and recommended procedure execution options.
  - Retracing of sequences of steps (selected procedure sequences), NOT including actions taken by the operator to control components, to ensure the proper status of components or systems is maintained.
  - Procedure validation on each operating procedure using the plant simulator

- ***Tech Spec Monitoring (TSM)***

  TSM provides for:

  – Warning the operator when a Limiting Condition of Operation (LCO) is being approached.

  – Warning the operator when an LCO is being violated.

  – Determining the approach to an LCO based on information on equipment status, core limits and margins and other data.

  – Indication, to the extent practical, of appropriate action(s) to avoid violating LCOs.

  – Acquisition and processing of available information needed to determine the approach to and existence of an LCO.

  – Automatic acquisition of required available information.

  – Determining, given available information, of any automatic testing that could impact LCOs.

  – Indication, to the extent practical, of the action needed to recover from an LCO.

  – Logging of all LCO violations.

  – Acquisition or calculation, as necessary, of reactor and core parameters required for monitoring LCOs, such as thermal margins, power distribution, heat generation rates, etc.

  – Showing the results of calculations of reactor and core parameters on operator displays.

  – Manual input capability for LCOs that cannot be monitored automatically by the TSM function.

  – Send alarms to the AAS, which shall provide for an acknowledgment function for alarm conditions.

  – Showing the operator the status of both the long term and short-term availability of the RPS and safety systems.

  – RPS and safety system monitoring (RPSM) as a sub-function.

  – Monitoring, through RPSM, of support services (e.g., voltages, cooling water, oil pressure and levels, etc.) that can affect the availability of the RPS and safety systems.

  – Monitoring, through RPSM, of the availability of both the initiating equipment (sensors, control systems, etc.) and the implementing equipment (pumps, valves, etc.).

  – Monitoring, through RPSM, of the availability of both primary and backup sources of services.

- Monitoring, through RPSM, of process parameters (reactor pressure, water storage tank levels, environment, etc.) that can impact the successful operation of the RPS or a safety system.

Monitoring, through RPSM, of the maintenance, calibration and test data needed to establish RPS and safety systems operability.

- ***3 D MONICORE***
  - 3D MONICORE has two major components, the Monitor and the Predictor. Both components use a three-dimensional core model code such as PANAC11 (or the current core model available for the ESBWR) as the main calculation engine. 3D MONICORE provides the logic in the input preparation file to interface with the core model code that calculates the key reactor state information such as axial and radial power, moderator void and core flow distributions. From these, other parameters such as the magnitude and location of minimum margin to thermal limits (such as minimum critical power ratios, peak fuel rod linear powers and average planar heat generation rates), fuel exposure and operating envelope data can be determined.
  - The 3D MONICORE Monitor is designed to periodically track current reactor parameters automatically with plant live data. Typically, the tracking interval is once per hour. The Predictor runs upon user request with live data overlaid with user input. It predicts core parameters for reactor states either in steady or operational transient states other than the present one. This allows the user to study the effects of different rod patterns, core flows and fuel burnups before performing reactor maneuvers to support plant operation.
  - For accuracy improvement, 3D MONICORE has several adaptation modes, which use in-core neutron flux measurements and gamma thermometer data to calculate nodal fit coefficients that may be input to later Monitor and Predictor cases. The choice of adaptation mode depends on the method used to adapt the results of the core model code to in-core detector measurements.
  - The 3D MONICORE function provides data to other systems including
  - Automatic Thermal Limits Monitoring (ATLM), Power Range Neutron Monitoring (PRNM) and Rod Control Information System (RC&IS). The data needed by these systems is detailed in their respective system specifications.
- ***Historian***
  - The Historian is the repository for all point data for the plant. It receives data from the various sources of point data. It stores this data and presents the data to the report generator, the display driver, and other applications needing historic point data.
  - The historian stores 3D MONICORE data in a format compatible for the display and report system. It is able to generate the data set in the format transferred from 3D MONICORE to the historian.
  - The on-line capability is, at a minimum, one month for the short-term data and three months for the long-term data. The system warns the system operator for disk space

problems, leaving enough time for download to an off-line archiving device, preferably optical disks.

- ***Transient Recording and Analysis (TRA) and Sequence of Events (SOE) Recording***
  - The TRA utilities are largely reports of current point and historical point data. The TRA utilities may be used to analyze plant events and to support plant startup tests.
  - Some analysis functions are triggered by plant events and periodically based on the wall clock (for example hourly, shift, daily logs and reports).
- ***Core Thermal Power and Core Flow Calculation***

  Calculates real time core thermal power from critical to 100% power. The calculation is supported by multiple parameter measurements and constants are normally used so that bias in the calculation is eliminated. At low thermal power levels the LFCV feedwater flow measurement is used to increase accuracy. The core flow is calculated by the heat balance core flow methodology, using the core inlet temperature measurement as inputs to determine core inlet enthalpy.
- ***Thermal Performance Monitor and Diagnostic (TPM&D)***
  - The TPM&D will provide on-line diagnostic and monitoring program for the thermal heat cycle. It will calculate the deviations from the calculated performance of individual system components compared to the actual measured performance when the plant is above some threshold power. The trends of the performance data may be used by utility personnel to identify components that may be contributing to thermal efficiency loss.
  - The Thermal Performance Monitor is a plant model that is normalized to current plant conditions such as reactor power, core flow, reactor pressure and circulating water temperature. The output of the model is a detailed calculation (flows, enthalpies, pressure, temperatures, etc.) of the plant individual heat cycle components predicted (design basis) and actual performance parameters under that condition. These actual and predicted parameters are compared, and their difference is used to calculate a figure of merit (example: equivalent system parameter such as normalized heat exchanger cleanliness).
- ***Report Generator (RP)***
  - The RG is a general-purpose report definition and execution utility program that allows the user to create reports within the PCF. It generates various required custom output reports in the MCR, TSC, and EOF.
  - The data sources for the RG include any measured or calculated data stored either in Historian or in the Real-time Database (measured and calculated points) that enables the report program to locate and retrieve data for pre-configured reports used by operators, engineers and maintenance personnel.
  - The RG is able to handle equations to support T/G and BOP supplier logs and reports.

- ***Plant Configuration Database (PCD)***
  - PCD provides overall configuration and management functions at an engineering workstation for the PCF
- ***Selected Control Rod Run-In (SCRRI)***
  - NE-DCIS will accept the redundant loss of feedwater heating signal from Feedwater Control System (FWCS) and the turbine trip and load reject signals from the turbine control system, performs 2/3 voting on each and combine them as an "OR" function to become the automatic SCRRI command signal. It will also be possible to initiate SCRRI manually from the main control room, which is part of the RC&IS (C11) system scope (i.e. the manual SCRRI function is implemented to be independent of NE-DCIS equipment scope).
  - The redundant NE-DCIS SCRRI command signals will be sent to RC&IS where each of the dual Rod Action and Position Information (RAPI) channels will perform a 2/3 vote and initiate RAPI channel logic associated with accomplishing the SCRRI function, which when activated, inserts control rods using the Fine Motion Control Rod Drive (FMCRD) motors to pre-defined positions to reduce reactor thermal power to a target power level. This logic will be implemented in a highly reliable redundant control system. The SCRRI command signal is also used in the Emergency Rod Insertion Control logic of NE-DCIS, as discussed below.
- ***Alternate Rod Insertion (ARI)***
  - NE-DCIS will accept the redundant "all rods insertion" signals from the Diverse Protection System (DPS) and perform 2/3 voting of these signals to become the NE-DCIS scope ARI initiation signal. Redundant ARI command signals will be sent to the RC&IS where each of the dual RAPI channels will perform a 2/3 vote and initiation RAPI channel logic associated with accomplishing the ARI (motor run-in) function.
  - When activated, ARI inserts all operable control rods to the normal full-in position, as a backup means for inserting all control rods automatically to the hydraulic ARI function of the CRD system. This logic will be implemented in a highly reliable redundant control system.
  - The ARI command signal is also used in the Emergency Rod Insertion logic of NE-DCIS, as discussed below.
- ***Emergency Rod Insertion***
  - NE-DCIS will combine the NE-DCIS SCRRI command signal and the NE-DCIS ARI command signal by an "OR" function to become an FMCRD emergency insertion signal. Redundant FMCRD emergency insertion signals are sent to the emergency rod insertion control panel of the RC&IS, which performs 2/3 voting. It will initiate associated emergency insertion condition signals of the emergency rod insertion panels of the RC&IS that provide inputs to the induction motor controllers (IMCs) of the RC&IS.

– For the SCRRI or ARI motor run-in function of the RC&IS equipment to be initiated, the emergency insertion signals to the IMCs must also be activated concurrent with the IMCs receiving the SCRRI or ARI related command signals transmitted from the RAPI logic. This logic will be implemented in a highly reliable redundant control system.

NE-DCIS has no safety-related function. The NE-DCIS performs the following nonsafety-related functions:

- Acquires process measurement and equipment status signals from the process sensors and discrete monitors of the plant's non safety-related systems.
- Performs signal conditioning and analog-to-digital (A/D) conversion for continuous process (analog) signals. NE-DCIS performs signal conditioning and change-of-state detection for discrete signals.
- Provides data message formatting and transmission of data from remote locations in the plant to the MCR via both fiber optic and hardwire network connections.
- Receives command and control signals from the redundant controllers in the MCR area, and transmits the signals from the MCR area to remote locations in the plant where NE-DCIS distributes the signals to the final actuating devices.
- Provides datalink interfaces to all control and logic processing equipment supplied by parties other than the primary NE-DCIS equipment supplier.
- Provides data support functions [e.g., Technical Support Center (TSC), Emergency Operations Facility (EOF)], and provides operator aids provided by the plant computer function of NE-DCIS, such as safety parameter displays, transient data recording, analysis, and archiving, alarm processing, and sequence of events processing.

In addition to the functions outlined above, the NE-DCIS also collects selected safety-related signals through isolated divisional interfaces for archiving and for nonsafety-related control and monitoring purposes. These gateways or workstations are always interconnected by fiber optics to provide the required isolation function. NE-DCIS has no control-related inputs to the safety system with the exception of Neutron Monitoring System (NMS) for Local Power Range Monitor (LPRM) and Average Power Range Monitor (APRM) calibration functions.

The NE-DCIS main data path consists of high-speed fiber optic paths to/from the RMUs in the field to the dual / triple redundant controllers located in the Control Building (CB). NE-DCIS has the following major equipment:

- Remote Multiplexing Units - The RMUs are located throughout the various plant buildings (such as Reactor Building, Control Building, Turbine Building, Radwaste Building, etc.). The RMUs acquire and output the same signal types as the E-DCIS RMUs but are nonsafety-related. The RMUs connect to the Network Switch Cabinets in the Control Building via redundant fiber optic links;
- Control Processor (CP) Cabinets – CP Cabinets house the dual / triple redundant control processors which process the control logic of non safety-related NSSS systems and most BOP systems. CP Cabinets receive plant process data multiplexed at the RMUs and transmitted through the Network Switch Cabinets to CP. They also transmit resulting

data to the RMUs for control purposes or the redundant high speed fiber optic networks for operator interface displays or plant-level applications;

- Network Switch Cabinets - Network Switch Cabinets contain switches for Ethernet switching, segmentation, and connection between all NE-DCIS components connected to the redundant high speed fiber optic networks;
- NE-DCIS Datalink Interfaces – NE-DCIS Datalink interfaces provide NE-DCIS communication interfaces with the Turbine Control System, Feedwater Control System, Steam Bypass & Pressure Control System, Plant Automation System – Automatic Pressure Regulator function, the Triple Modular Redundant (TMR) systems, and other packaged systems.

7.9.2.2 System Description

The NE-DCIS provides distributed and control (I&C) data communication networks to support the monitoring and control of interfacing nonsafety-related plant control and instrumentation systems. The system includes electrical devices and circuitry (such as remote multiplexing units, control processors, network switches, data communication paths and interfaces) that connect field sensors, display devices, controllers, power supplies, and actuators, which are part of the nonsafety-related systems. The NE-DCIS also includes any associated data acquisition and communications software, if required, to support its data distribution and control function. The system processes data from and for nonsafety-related systems through the NE-DCIS itself, while E-DCIS safety-related data is processed through the E-DCIS. Nonsafety-related data from E-DCIS to NE-DCIS is always transmitted through optical fiber to provide the required isolation between the safety and non-safety DCIS.

NE-DCIS replaces most of conventional, long-length, copper-conductor cables with a dual or triple redundant, fiber optic, data network. Triple redundant data network is implemented within specific plant systems (such as feedwater control system, steam bypass and pressure control systems, and plant automation system – automatic power regulator function) to improve reliability and online diagnostics and maintenance. The fiber optic data network reduces the cost and complexity of cable runs and provides an electrically noise-free transmission path for plant sensor data and nonsafety-related control signals.

The nonsafety-related data from sensors are multiplexed at nonsafety-related remote multiplexing units (RMUs) and then transferred via the NE-DCIS data network to various components of the NE-DCIS. Selected signals from the nonsafety-related instrumentation are transmitted to NE-DCIS input cabinets via dedicated hardwired connections as required for faster transmission rates of signals. Similarly, output signals to actuators and controls requiring faster transmission rates also utilize dedicated hardwired connections. The RMUs and the data communication network for such nonsafety-related data processing and transmission are part of the NE-DCIS.

There are divisionally separated redundant isolated digital gateways to provide one-way communications from safety-related systems to the NE-DCIS. This gateway function is part of the safety E-DCIS. The communication from nonsafety-related systems to E-DCIS is limited to communication from the 3D Monicore function of the NE-DCIS to the PRNM (LPRM and APRM) function of the Neutron Monitoring System (NMS).

Refer to section 7.9.1.2 for time tagging of data from E-DCIS to NE-DCIS.

The local NE-DCIS RMUs perform signal conditioning and A/D signal conversion for continuous process signals, and perform signal conditioning and change-of-state detection for discrete signals such as contact closures/openings. The RMU function can be applied for performing both input and output signal processing functions. The RMU formats the acquired signals into data messages and transmits the data via the data network to various NE-DCIS components for logic processing. The RMU with a system logic function then receives various logic commands (such as trip commands and control signals) from the data network NE-DCIS logic processors. The RMU then provides terminal points for distributing the signals to the final actuating devices of the nonsafety-related systems.

Operator interfaces for control and display is realized through multiple, non-dedicated touch-screen visual display units (VDU), each of which is connected to the network. An illustration of a typical NE-DCIS network and associated components and links are shown in Figure 7.1-1.

NE-DCIS contains on-line diagnostic functions that monitor transmission path quality and integrity. The dual redundant data communication paths are repairable on-line if one path fails. NE-DCIS failures are alarmed in the MCR. Periodic surveillance, using off-line tests with simulated input signals, may be used to verify the overall system integrity.

The NE-DCIS networks are distributed throughout the plant and are powered by redundant and triple redundant (specific systems such as TCS, FWC, SB&PC, and PAS-APR) internal power supplies from two or three non-safety related load groups (as applicable) of the 120 VAC Vital AC uninterruptible power system.

NE-DCIS has no safety-related function.

System Configuration

The system includes electrical devices and circuitry, such as Remote Multiplexing Units (RMUs), Control Processors (CP), Network Switches, communication interfaces, and power supplies, that connect field sensors, display devices, controllers, power supplies, and actuators, which are part of other plant systems. NE-DCIS also includes the associated data acquisition and communications software required to support its distribution function of plant-wide data and control. Nonsafety-related data is processed through NE-DCIS.

The following major items comprise NE-DCIS:

- RMU cabinets for Non-Class 1E Input/Output (I/O) with built in RMU internal bus and power supply modules that accept two sources of nonsafety-related 120 VAC
- Dual redundant controllers in the MCR area to provide for all specified I/O and control algorithms
- Gateway associated with the triple redundant controllers in the MCR back panel area
- CP Cabinets to enclose the nonsafety-related control processors in the MCR.
- Network Switch Cabinets house network switches in MCR area.
- Fiber optic cabling for Non-Class 1E Fast Ethernet and redundant fiber optic cables in the field

- Signal Isolators for RMU internal bus and the redundant fiber optic links in the field
- I/O modules to provide interface between process sensors/actuators
- Fiber optic modems to transmit and receive data via the redundant fiber optic links in the field to the redundant control processors
- Gateway devices, or workstations, convert the data from E-DCIS to be transmitted into the needed data transmission format usable by the NE-DCIS.
- Datalink interfaces provide communications between NE-DCIS and non safety-related plant systems supplied by parties other than the primary NE-DCIS equipment supplier.
- E-DCIS Datalink interfaces provides communications specifically required from the E-DCIS to the NE-DCIS.
- **NE-DCIS provides information to the Large** Display Panel (alarm display, mimic, flat panel displays, CCTV monitors, large variable display, and their associated computer processors). The large display panel is part of Main Control Room Panels.
- **NE-DCIS provides information to the nonsafety-related portion of the** Main Control Room Consoles (flat panels w/soft controls, hard controls, page/party phone, meters, silence/acknowledge, recorders, main gen. synchronizing inset, PAX phone, radio handsets, keyboards/trackballs, etc.) The main control room consoles are part of the Main Control Room Panels.
- Computer peripherals, such as printers and plotters, used for data printing capabilities.

Hardware Configuration

The NE-DCIS main data path consists of high-speed fiber optic paths to and from the RMUs in the field to the dual / triple redundant controllers located in the Control Building (CB). (The communication from safety-related systems and E-DCIS has their own gateways to transmit the data to NE-DCIS.) Main equipment of NE-DCIS, as described in Subsection 7.9.2.1, includes: Remote Multiplexing Units, Control Processor (CP) Cabinets, Network Switch Cabinets, NE-DCIS Datalink Interfaces with other control systems, and NE-DCIS Computer Peripherals such as printers and plotters for data printing capabilities.

7.9.2.3 Safety Evaluation

The NE-DCIS is classified as a primary data communication system with power production applications and is not required for safety purposes, nor is it required to operate during or after any design basis accidents. The system is required to operate in the normal plant environment and is essential to data communications and power production applications. NE-DCIS does not perform any safety-related functions as a part of its design; however the NE-DCIS does provide an isolated alternate path for safety-related data to be presented to the plant operators. The NE-DCIS network that supports the dual/triplicate, fault-tolerant controllers of the process control systems uses a different and proven technique for high speed transfer of data other than the E-DCIS and thus provides diversity in design.

The NE-DCIS equipment is located throughout the plant and is subject to the environment of each area. Typical locations are:

- RMUs – Located throughout the plant and auxiliary buildings
- Computer equipment and peripherals – Located mainly in the Control Building – Main Control Room and Back Panel areas; other typical areas such as Emergency Operations Facility, Radwaste Building, and Technical Support Center, Auxiliary Fuel Building, Auxiliary Fuel Building roof area, or alternate building designations specific to the plant design

The NE-DCIS panels and components are designed for retaining structural integrity as to not impair any safety-related equipment in its area from performing its safety function.

Table 7.1-1 identifies the NE-DCIS and the associated codes and standards applied in accordance with the Standard Review Plan (SRP) 7.9. The following analysis lists the applicable criteria in order of the listing on the table, and discusses the degree of conformance for each. Any exceptions or clarifications are so noted.

10 CFR Part 52

52.47(a)(1)(iv) Resolution of Unresolved and Generic Safety Issues

Conformance: NE-DCIS system is nonsafety-related and conforms in that there are no unresolved issues for the NE-DCIS system. Resolution of unresolved and generic safety issues is discussed in Section 1.11.

52.47(a)(1)(vi) ITAAC in Design Certification Applications

Conformance: Test, inspection, analyses, and acceptance criteria of the NE-DCIS are identified in Tier 1.

52.47(a)(1)(vii) Interface Requirements

Conformance: Design interface requirements during the licensing certification and design phases shall be commensurate with the detail required to support completion of the final safety analysis and design-specific probabilistic risk assessment. Interface material is provided in Tier 1.

52.79(c) ITAAC in Combined Operating License Applications

Conformance: NE-DCIS system is nonsafety-related and conforms to those sections applicable for test, inspection, analyses, and acceptance criteria of the NE-DCIS, as identified in Tier 1.

General Design Criteria

Criteria: GDC 13, 19, and 24

Conformance: The NE-DCIS is in conformance with the GDC identified above. Refer to Subsection 3.1.2 for general discussion of the GDC.

Additional Acceptance Criteria Applicable To ALWR Annunciator Systems

Staff Requirements Memorandum (SRM), SECY-93-087, Item II.T, Control Room Annunciator (Alarm) Reliability – Refer to Section 7.5 for compliance discussion.

Conformance: The NE-DCIS alarm system meets the intent of the EPRI requirements for redundancy, independence, and separation in that the "alarm system" is considered redundant.

- Alarm points are sent via dual network to redundant message processors on dual power supplies. The alarm processors are dedicated and redundant and conservatively sized.

- The alarms are displayed, on multiple independent VDUs (dual power supplies on each).
- The alarm tiles are driven by redundant datalinks to the alarm tiles (dual power). The alarm tile processor is redundant.
- Each alarm tile has at least two "bulbs" (LEDs) of each color.
- The only thing that is not redundant is the horn and voice speaker. Test buttons are available to test the horn(s) and all the lights.
- There are no alarms requiring manually controlled actions for safety systems to accomplish their safety function.

Regulatory Guides

Regulatory Guide 1.151, Instrument Sensing Lines

Conformance: Not applicable to the NE-DCIS system. The NE-DCIS receives signals from sensors in various systems in the plant that are from instrument sensing lines from nonsafety-related instrumentation but the system itself does not contain instrument sensing lines.

Branch Technical Positions

BTP HICB-14: Guidance on Software Reviews for Digital Computer-based Instrumentation and Control Safety Systems

Conformance: See APP.7B discussion. NE-DCIS conforms to the intent of this guideline as outlined in ISO 17799 for Security Management of the NE-DCIS Control Network.

BTP HICB-16, Guidance on Level of Detail Required for Design Certification Applications Under 10 CFR Part 52

Conformance: The level of detail is commensurate with this BTP.

Regulatory Guides (RGs)

In accordance with the SRP for 7.9, and with Table 7.1-1, there are no RGs specified for NE-DCIS.

From the foregoing analysis, it is concluded that the NE-DCIS meets its design bases.

7.9.2.4 Testing and Inspection Requirements

The NE-DCIS controllers input and output communication interfaces are continuously functioning during normal power operation. Abnormal operation of these components can be detected during operation. In addition, the controllers are equipped with on-line diagnostic capabilities for identifying and isolating failure of input/output signals, buses, power supplies, processors, and inter-processor (IO Net) communications. These on-line diagnostics can be performed without interrupting the normal control operation of the NE-DCIS system by removing one of the redundant paths from operation.

The NE-DCIS components and critical components of interfacing systems are tested to assure that the specified performance requirements are satisfied. Preoperational testing of the NE-DCIS

is performed before fuel loading and startup testing to assure that the system functions as designed and that stated system performance is within specified criteria.

7.9.2.5 Instrumentation Requirements

Power Sources

Uninterruptible Nonsafety AC Power Supply

The uninterruptible nonsafety AC power is an uninterruptible power source normally supported by AC power. However, if off-site power fails, it receives power from a DC source (batteries). NE-DCIS has three redundant nonsafety AC uninterruptible power supplies of 120 ±10% volt AC, 60 Hz and three corresponding separate battery systems. NE-DCIS panel design is such that loss of one power supply or incoming power source shall not affect NE-DCIS system functional operation and thus plant operation.

Lighting and Service Power System (LSP)

LSP supplies 120 VAC to NE-DCIS for lighting and maintenance equipment.

Major instrument interfaces with NE-DCIS

NE-DCIS has interfaces with almost all of the nonsafety-related plant systems; safety-related system information acquired by E-DCIS is also available in NE-DCIS. System interfaces with nonsafety-related systems, or portions of systems, and data acquisition of E-DCIS data through isolation devices/gateways include:

- Nuclear Boiler System
- Isolation Condenser System
- Rod Control and Information System
- Control Rod Drive System
- Leak Detection and Isolation System
- Feedwater Control System
- Standby Liquid Control System
- Neutron Monitoring System
- Remote Shutdown System
- Essential Distributed Control and Information System
- Reactor Protection System
- Safety System Logic and Control
- Plant Automation System
- Steam Bypass and Pressure Control
- Process Radiation Monitoring System
- Area Radiation Monitoring System

- Gravity-Driven Cooling System
- Fuel Transfer System
- Fuel and Auxiliary Pools Cooling System
- Reactor Water Cleanup and Shutdown Cooling System
- Diverse Protection System
- Liquid Waste Management System
- Solid Waste Management System
- Offgas System
- Turbine Main Steam System
- Condensate and Feedwater System
- Heater Drain and Vent System
- Condensate Purification System
- Main Turbine
- Turbine Control System
- Turbine Gland Seal System
- Turbine Lubricating Oil System
- Moisture Separator Reheater System
- Extraction System
- Turbine Bypass System
- Turbine Auxiliary Steam System
- Generator
- Hydrogen Gas Cooling System
- Generator Cooling System
- Generator Sealing Oil System
- Main Condenser and Auxiliaries
- Circulating Water System
- Makeup Water System
- Reactor Component Cooling Water System
- Turbine Building Cooling Water System
- Chilled Water System
- Condensate Storage and Transfer System

- Oxygen Detection System
- Process Sampling System
- Plant Service Water System
- Service Air System
- Instrument Air System
- High Pressure Nitrogen Supply System
- Auxiliary Boiler System
- Hydrogen Water Chemistry
- Zinc Injection System
- Post Accident Sampling
- Electrical Power Distribution System
- Medium Voltage Distribution System)
- Low Voltage Distribution System
- (Uninterruptible) AC Power Supply
- Instrumentation and Control Power Supply
- Lighting and Servicing Power Supply
- Direct Current Power Supply
- Standby On Site AC Power Supply
- Passive Containment Cooling System
- Containment Inerting System
- Drywell Cooling System
- Flammability Control System
- Containment Monitoring System
- Electric Equipment Building HVAC
- Service Building HVAC
- Radwaste Building HVAC
- Turbine Building HVAC
- Reactor Building HVAC
- Fire Protection System
- Equipment and Floor Drain System
- Control Building HVAC

- Fuel Storage Building HVAC
- Service Water and Fire Building HVAC
- Meteorological Observation System
- Yard Miscellaneous Drain System
- Oil Storage and Transfer System

(Typical Division)

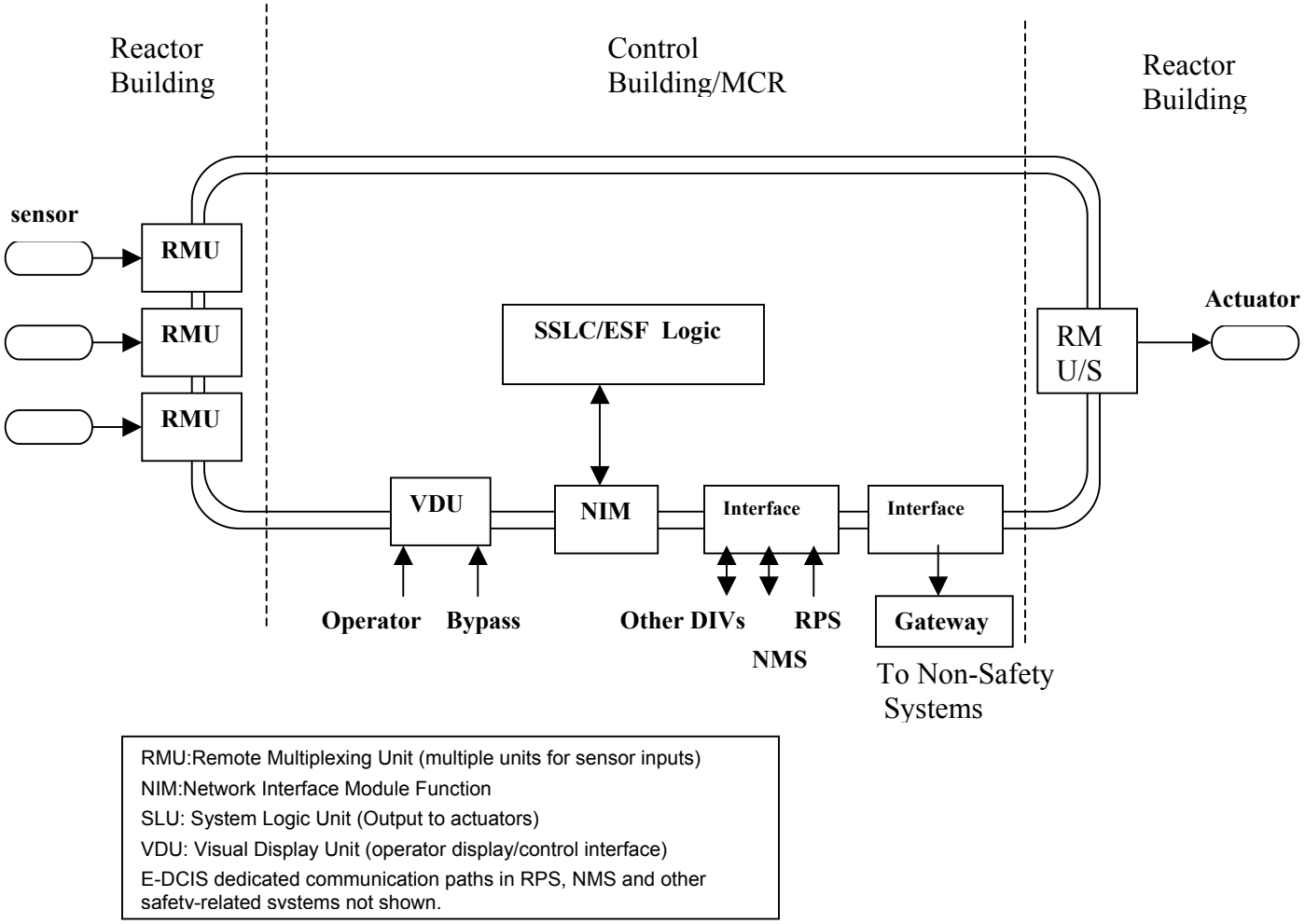


Figure 7.9-1. E-DCIS with SSLC (ESF) Components

7A. FIXED IN-CORE CALIBRATION SYSTEM FOR THE NEUTRON MONITORING SYSTEM

7A.1 INTRODUCTION

7A.1.1 Objectives

The ESBWR Neutron Monitoring System (NMS) is improved over previous BWR NMSs through the replacement of the conventional source range monitor (SRM) and intermediate range monitor (IRM) with the startup range neutron monitor (SRNM), the optimization of the local power range monitor (LPRM) instrument configuration, and the replacement of the conventional traversing in-core probe (TIP) system with a fixed in-core calibration system. This system utilizes Gamma Thermometers (GT) installed within the individual LPRM assemblies to provide an independent and stable indication of the local core power levels. Such local power data are then provided as input to the plant process computer for the three-dimensional core power calculation and LPRM calibration.

This appendix contains the design and operation principles as well as the operation experience of GTs in BWR plants. The design of the integrated LPRM and GT assembly for the ESBWR is also described together with a discussion on the estimated ESBWR local core power calculation accuracy based on the GT design.

Finally, the reliability and other mechanical and electrical considerations of the GT are also discussed.

7A.1.2 Principles of the Gamma Thermometer

The ESBWR GT is a metal rod that is heated by the gamma rays generated within the reactor core. The heat generated is proportional to the specific power of adjacent fuel rods. Heat generated within the GT metal mass escapes to a heat sink through a controlled heat path.

The temperature differential developed along that heat path is directly proportional to the rate of heating caused by the impinging gamma rays. Therefore, the temperature differential is proportional to the power generated in the adjacent fuel rods. A differential thermocouple embedded in the GT measures the temperature differential along the controlled heat path and produces a voltage signal that is proportional to the local core power level.

Because the GT design does not involve any fissile material, there is no decrease in the detector sensitivity as a result of radiation exposure such as that associated with the LPRM fission chambers. With their simple operating principles, GTs have a very low failure rate (Reference 7A-1).

7A.1.3 Summary of Gamma Thermometer Application in All BWRs

GTs have been used for reactor local power measurements for over forty years. Early applications of GTs showed acceptable performance results in heavy water reactors in the U.S. at Savannah River and at the Halden reactor in Norway (Reference 7A-1). Later on, GTs were also extensively tested in many light water reactors throughout the nuclear industry (Reference 7A-1 and Reference 7A-2). This includes demonstrations performed at Limerick 2 in the U.S., Tokai 2 and Kashiwazaki-Kariwa 5 in Japan.

In the ESBWR, the LPRM provides the safety protection function through local power monitoring, while the GT provides information for core power calculations and for calibration of the LPRMs. By incorporating the fixed in-core GTs as the means for performing LPRM calibration, the entire TIP system is eliminated in the ESBWR design. This is consistent with the ESBWR design goal of easier operation and maintenance.

The fixed in-core GTs are installed within the LPRM assemblies. There is one GT permanently installed next to each of the four individual LPRM detectors, so that the output signals from the GTs and the LPRM detectors can be easily compared. The GT signal cables are routed to the electronics unit through the LPRM assembly penetrations in the lower head of the reactor pressure vessel.

In the ESBWR NMS design, the GTs provide the primary inputs required for the periodic core power calculation and LPRM calibration. With the incorporation of the GTs, acquisition of the local core power data can now be completed almost instantaneously. This capability to acquire all of the data simultaneously offers a significant improvement over the operation of a conventional TIP system, which can take hours to acquire a full core set of TIP data.

With automation of the entire process from the initiation of the GT data acquisition to the performance of the core power calculation and LPRM calibration, execution of the standard periodic data acquisition and LPRM calibration can now be completed more frequently and with minimum operator effort. The operational time interval between each subsequent whole core GT scan is significantly reduced, compared to that using a TIP system. The LPRM calibration interval is also significantly reduced. A direct advantage of the increased frequency of those periodic updates is that the accuracy of the core power calculation and LPRM readings are improved.

7A.2 GAMMA THERMOMETER SYSTEM DEFINITION

7A.2.1 Hardware Description

The hardware configuration for a typical GT core monitoring system includes new components such as the LPRM/GT assemblies, the Data Acquisition System (DAS) and the Heater Power Supplies (HPS). A listing of the new components is provided in Table 7A-1. Also listed is the number of each type of component that is required for a complete system.

LPRM/GT Assembly

The LPRM/GT assemblies are similar to standard LPRM assemblies: each has four LPRMs and was designed to meet all of the normal requirements. In the ESBWR configuration, each assembly has four GTs. In other designs, up to nine GTs are possible. In the nine GT configuration, the GTs are positioned as follows: one adjacent to each LPRM, one midway between each pair of LPRMs, one midway between the bottom of the core and the lowest LPRM and finally, one midway between the highest LPRM and the top of the core.

There are many requirements that the GT sensors must meet. For example, the range in gamma heating rate should be 0.0 to 2.4 W/g for a typical BWR. In addition, the GT sensitivity at beginning of life at operating temperature (286°C) should be 1.5 mV-g/W ±20%.

The environmental design ratings, including the operating temperature, neutron flux, gamma dose rate and seismic loadings are the same as for standard LPRM assemblies. The GT sensors are designed to last at least as long as the LPRMs.

For demonstration systems only, a calibration tube is included in the assembly so that the TIP system remains fully operational. This permits a direct comparison between the TIP and GT systems.

Data Acquisition System

The main function of the Data Acquisition System (DAS) is to transform the GT readings from an analog signal to a digital value. The environmental design ratings are similar to other electronics in the reactor building. In additional, the DAS system performs digital filtration to remove noise as well as digital compensation to account for delayed gammas.

Heater Power Supply

The purpose of the Heater Power Supply (HPS) is to provide a DC electrical current to the internal GT heaters during calibration. The current must be of sufficient magnitude to allow an accurate calibration of each GT sensor. The HPS, for economic reasons, is multiplexed such that several GT assemblies are serviced sequentially by a single power supply. The HPS are included in the DAS cabinets.

GT Control Cabinet

The GT Control Cabinet contains an Engineering Work-Station (EWS) that is the principal interface to the GT system. It provides a manual way of initiating the GT calibration and in addition provides color graphic displays of all useful output: GT readings, GT sensitivities and others.

The EWS communicates with the other units including the DAS and ATLM cabinets through a fiber optic link.

7A.2.2 Software Description

The software for the GT Core Monitoring System consists of four main modules: a GT monitor and signal conditioning module, a GT calibration module, a 3D Simulator, and a User interface module. Each of these modules is described in the sections that follow.

GT Monitor Module

The GT monitor module, GTMON, is responsible for conditioning the GT signals. This conditioning will occur continuously while the reactor is in operation. The time step for digital filtration will be one second or less. The specific functions of GTMON are as follows:

(1) Digitally filter the GT signals (a typical time constant is 8 seconds)

(2) Perform delayed gamma compensation on the filtered GT signals

(3) Digitally filter the GT heater current and voltage readings during GT calibration

(4) Block transmittal to the 3D Simulator (or otherwise mark as unusable) GT signals associated with GT strings that are being calibrated

GT Calibration Module

The GT calibration module, GTCAL, is responsible for maintaining the accuracy of the system by initiating calibration of the GTs at appropriate times. This initiation is automatically performed, or it may be requested by the User. The specific functions of GTCAL are as follows:

(1) Calibrate the GTs (every 200-1000 hours; more frequently when the GTs are new)

(2) Initiate the GT calibration by turning on the Heater Power Supplies

(3) Closely monitor and record the GT sensor readings during calibration

(4) Calculate the sensitivity constants So and the extrapolation constants a, b and g that are used for estimating the change in GT sensitivity with time

3D Simulator

The 3D Simulator is responsible for calculating the core power distribution and the associated thermal limits, such as the critical power ratio and the linear power density. Some of the specific functions are:

(1) Compute the core power, void and exposure distributions

(2) Adapt the power distribution to the current GT readings

(3) Calculate calibration constants for the LPRMs

(4) Adapt to the LPRMs (if necessary, due to plant transient state)

(5) Compute GT and LPRM exposures

User Interface

The User interface is responsible of accepting User command input and displaying calculated results in the most useful possible way. Some of the major functions of the User interface are:

(1) Accept User commands

(2) Provide color graphic displays

(3) Initiate GT calibration (on demand)

(4) Initiate 3D simulation (on demand)

(5) Display calibration results

(6) Display simulation results

7A.3 GAMMA THERMOMETER SYSTEM FUNCTIONS

7A.3.1 LPRM Calibration

LPRM calibration is the process of adjusting LPRM readings to match a standard. In early core monitoring systems, the standard was a neutron TIP trace or an adjusted gamma TIP trace. In modern systems, such as 3D MONICORE™, the standard consists of calculated LPRM readings, which are based on a power distribution that has been adapted in some way to the distribution of neutron and gamma TIP readings. In a GT system the process is the same except that the power distribution is adapted to the GT sensor readings instead of a TIP trace.

One very significant feature of a GT system is that the GT readings are always available. Therefore, an LPRM calibration can be performed at any convenient time.

As estimated by the core monitor, the LPRM sensor reading at elevation l in string s is determined by averaging estimates from each of the four surrounding fuel nodes:

$$LPRM_{ls} = \tfrac{1}{4}\sum_{n=1}^{4} R_n^{th} P_n$$

where P_n is the nodal relative power and R^{th}_n is the sensor-to-power ratio, which is evaluated from a correlation in the control fraction, exposure, relative water density and historical water density. The theoretical detector gains are simply the ratio of the calculated to measured readings:

$$GAIN_{ls} = LPRM_{ls} \big/ LPRM_{ls}^{Meas}$$

7A.3.2 Core Monitoring with Gamma Thermometers

Adaption is the process by which the nodal power distribution in the core is adjusted to conform to a set of measurements. The measurements can be LPRM readings, TIP traces or in the present case, GT readings.

In a TIP system, TIP adaptions are performed approximately every 1000 – 2000 hours. LPRM adaptions are performed in between.

In a GT system, on the other hand, GT adaptions are performed more frequently. The only caveat is that the plant must be operating in the steady state. It is optional whether or not LPRM adaptions are performed. For designs with more than 4 GT sensors per assembly, GT adaption is slightly more accurate than LPRM adaption and therefore LPRM adaption is not used. However, for designs with 4 GT sensors, the accuracy should be very close (provided the LPRMs are numerically recalibrated frequently—more frequently than is commonplace with TIP systems). In this case, LPRM adaption is performed.

For a gamma sensitive detector such as a GT, the calculated reading for sensor m in string s is:

$$GT_{ms} = \tfrac{1}{4}\sum_{n=1}^{4} R_n^{\gamma} P_n$$

where the sensor-to-power ratio R^{g}_n is determined by a correlation with the same form as for R^{th}_n, but with different coefficients.

There is more than one possible adaptive model that may be used. However, when the adaptive process is complete, the calculated GT readings from Equation 7A.3-3 are equal to the measured readings:

$$GT_{ms} = GT_{ms}^{Meas}$$

This process is referred to as absolute adaption. In a similar process called shape adaption, the readings for each string are normalized separately:

$$GT_{ms} \Big/ \sum_{l=1}^{l\,max} GT_{ls} = GT_{ms}^{Meas} \Big/ \sum_{l=1}^{l\,max} GT_{ls}^{Meas}$$

Either process is acceptable for GT adaption. Because GT readings are always available, GT adaption may occur far more frequently than TIP adaption (which typically occurs once a month). In most cases, GT adaption can be used in place of LPRM adaption, thus eliminating LPRM drift as one of the terms in the estimation of nodal power uncertainty.

7A.4 PRIOR EXPERIENCE WITH GAMMA THERMOMETERS

7A.4.1 Nuclear Industry Experience

The first gamma thermometer sensors were developed, manufactured, and used at the Savannah River Plant (SRP) in Aiken, S.C., from 1950 to 1980. These were single sensors approximately one inch in diameter. Although they represent the base technology for the present design Radcal Gamma Thermometer (RGT), their configuration is far enough removed in design that reliability comparisons are impractical.

Table 7A-2 summarizes the worldwide experience with gamma thermometers. Four single sensor RGTs were installed in Dodewaard, Netherlands, in 1980. They were much smaller in diameter than the SRP sensors and embodied many of the characteristics of the present design but also had many differences. The first RGTs of the present configuration were installed in Bugey-5, in France in 1979. From that time until the present there have been 86 RGTs supplied to various reactors with a total of 719 sensors.

Of 18 sensors in Bugey-5, several failed after some 3 – 4 years of service. The others are still operational. Of eight instruments with 72 sensors installed in Tricastin-2 and 3 in 1980, 3 sensors in Tricastin-2 have failed. All others are operating normally. One heater failed in Tricastin-2 also. Three of twelve sensors failed in Forsmark unit 1. However, all failed during installation. Two sensors have failed in each of the two units installed in ANO-2. It is believed that the failures were at least partially due to installation problems. One heater failed in a Ringhals unit 2 after two power cycles. All sensors are operational. One unit at the Consumer Power Palisades Plant experienced a heater and a single sensor failure. It was replaced in 1990 and is now fully operational. A second Palisades unit experienced one sensor failure.

Thus to date, three of 84 heaters (3.6%) and 19 of 719 (not counting four Dodewaard) thermocouples (2.6%) have confirmed failures. Some installations such as Savannah River have not yet operated all units while some units have been operational for over 10 years. Most failures occurred on the initial set of units installed so that early limited manufacturing experience appears to be a factor in failure rate.

7A.4.2 BWR Experience

There have been three in-plant tests of GT sensors in BWRs thus far. The first test was at Limerick 2 and lasted for two cycles, a total of four years. The second test, which was at Tokai 2, lasted for a single cycle of one year duration. These two tests will be described in detail in sections that follow. Published data from a third test at Kashiwazaki-Kariwa 5 are available in the open media and are summarized in section 7A.4.2.3

7A.4.2.1 Limerick 2 In-Plant Test

The Limerick 2 plant, operated by Exelon (formerly PECO Energy) is an 1100 MWe BWR4. It has 764 bundles arranged in a "C" lattice configuration (equal water gaps). It has a gamma sensitive TIP system with a total of 43 calibration tubes and associated LPRM strings.

7A.4.2.1.1 Test Plan

The LPRM/GT test program began in February 1995 with the installation of two Gamma Thermometer "strings" in the Limerick 2 core. Each GT string in the test consisted of four Gamma Thermometers, each of which was positioned adjacent to an LPRM. GT string number 1 was installed within LPRM string 37 at core location (32-49), while GT string number 2 was installed within LPRM string 31 at core location (40-41).

The calibration (TIP) tubes were left intact so that the TIP system would operate normally and so that a direct comparison could be made between the Gamma Thermometer and Gamma TIP readings. In a fully operational GT system, the calibration tubes are of course unnecessary.

The test plan called for automatically recording on a daily basis all of the GT readings and their corresponding LPRM readings. Whenever a TIP set was to be taken (normally every 1000 to 2000 full-power-hours), the GT calibration process was to be manually triggered and the GT, LPRM and gamma TIP readings automatically recorded.

The in-plant test was scheduled to last for two complete two yearlong fuel cycles. This is the equivalent of four annual cycles. The first cycle of the test program began in February 1995 and ended on January 30, 1997. The second cycle began on February 26, 1997 and continued until May of 1999.

7A.4.2.1.2 Hardware Description

The data acquisition system consisted of two Analogic ANDS4810 12 bit analog to digital (A/D) converters, one for each LPRM/GT assembly. Each module had eight inputs, six of which were used: four for the GT thermocouples, one for the heater current and one for the heater voltage. The fiber optic outputs from the A/D modules were fed to an ANDS4830 multiplexer and from there to the inputs of two data formatters, which communicate with the plant process computer.

The GT calibration system consisted of a GE FANUC 9030 Programmable Logic Controller (PLC) and two Lambda Electronics LMS-9300 power supplies. A manual push button switch attached to the PLC initiated the calibration. The PLC provided a suitably ramped input signal to each power supply to control the output currents at the prescribed levels. During the first 30 seconds, the current was ramped up from zero to one amp, held constant for 2.5 minutes, ramped up to two amps within 30 seconds and held constant for another 2.5 minutes, ramped up to 2.8 amps for a final 2.5 minutes and them ramped back downward to zero in 30 seconds. The three steps in the current allowed three separate estimates of the GT sensitivity. This allowed the investigation of possible non-linearity in the calibration process, but is not required in a production GT system.

7A.4.2.1.3 GT Calibration Results

The sensitivity of each thermometer showed the characteristic initial decline, followed by relatively steady operation.

The full power data include several calibrations performed after the restart for the second cycle of operation. It is clear from the data that the sensitivities (at full power) were unaffected by the shutdown and subsequent restart. This is contrary to the report from other researchers that GT sensitivities rose after a shutdown and then fell rapidly to their earlier level (Reference 7A-1).

The initial decrease in the GT sensitivity was very consistent among all eight of the GT sensors in the in-plant test. A model was developed to predict this behavior. This model is not essential for a production GT system, since GT calibration could be performed at more frequent intervals initially. However, use of such a model may reduce the need for calibration and may improve overall system accuracy.

7A.4.2.1.4 Comparison with Gamma TIPs

In general, a comparison of the GT sensor readings with gamma TIP readings was made whenever high quality (steady state, rated power) TIP data were available. A GT calibration was performed at the same time or soon after the TIP set so that the highest accuracy in the GT readings would be obtained. However, the GT readings were usually recorded twenty-four hours or more after the TIP set, because of practical considerations. This should not detract from the comparisons, because the plant was operating in the steady state in each case.

A comparison was made between the specific power in watts per gram of the four GTs in assembly 1 and the corresponding TIP readings. The TIP readings, which were available in twenty-four axial nodes, were interpolated to provide values at the exact elevations of the GTs and then normalized to the average specific power from the GTs (averaged over both assemblies). This re-normalization was necessary because the TIP readings, unlike the GT readings, are not absolute measurements, but relative values with an arbitrary normalization.

A similar comparison was made for GT assembly 2. In general, the GT readings and the TIP readings track each other very well. In cases where biases exist, they are generally unvarying with time. The statistical differences between each GT and its corresponding TIP readings are shown in Table 7A-3. The overall RMS difference between all readings is 4.5%.

A careful review of these data indicates that while all of the GTs are performing consistently, sensor D of GT2 has a large and consistent bias with respect to the TIP readings. This bias is believed to be due to factory calibration error.

7A.4.2.1.5 Conclusions

The test program completed two cycles (four years) of operation without a sensor failure. GT readings were recorded on a daily basis and calibrations were performed after TIP sets whenever practical.

The GTs performed quite well in general, although the differences with the gamma TIPs were somewhat larger than expected. Following this test, improvements in calibration methods were made such that GTs are expected in the future to achieve equivalent or superior accuracy relative to the current TIP system.

7A.4.2.2 Tokai 2 In-Plant Test

The Tokai 2 plant, operated by Japan Atomic Power Company (JAPC), is an 1100 MWe BWR5 with 764 fuel bundles arranged in a C lattice. It has a neutron sensitive TIP system with a total of 43 calibration tubes.

7A.4.2.2.1 Test Plan

The Tokai 2 In-Plant test began in April 1998 and was completed at the end-of-cycle in April 1999. The test was based on two LPRM/GT assemblies, each with nine GT sensors and four LPRMs. These LPRM/GT assemblies replaced standard LPRM assemblies in the Tokai 2 core during cycle 17.

The In-Plant test covered a wide variety of normal BWR operating conditions: from low power at startup, through full power, steady-state operation and concluding with power descent at end-of-cycle. The following is a list of the specific tests that were performed:

(1) Time dependence of GT sensitivity.

(2) GT sensitivity projection (future prediction of GT sensitivity).

(3) Steady-state GT response, converted to an equivalent neutron fission detector response, compared with neutron TIP response.

(4) Steady-state GT response, converted to an equivalent neutron fission detector response, compared with LPRM response.

(5) GT low power response, converted to an equivalent neutron fission detector response, compared with LPRM response.

(6) GT response, converted to an equivalent neutron fission detector response, compared with LPRM response during startup, flow change, control blade pattern change and power descent at end-of-cycle.

(7) GT transient response to internal heater during calibration.

(8) GT transient response to control blade movement.

(9) Comparison of the power distribution, determined from (adapted to) the GT readings, with the power distribution, determined from the neutron TIP readings.

(10) Comparison of the thermal limits (MCPR, MLHGR) determined from the GT readings, with the thermal limits determined from the neutron TIP readings.

7A.4.2.2.2 Hardware Description

The Data Acquisition and Calibration System (DACS), designed by Toshiba, consisted of the following hardware components:

(1) A Gamma Thermometer Monitoring Unit (GTM) with eighteen analog-to-digital converters for the GT thermocouple sensors plus additional converters for the heater current and voltage;

(2) A Heater Switching Unit (HSU) to switch the heater current from one GT assembly to the other, as needed or calibration;

(3) A Heater Power Supply (HPS) to deliver current to the GT internal heater wires for calibration;

(4) A Gamma Thermometer Control Unit (GTC) to provide a human interface to the GT system in order to trigger calibration and other functions; and

(5) A Data Logging Computer (DLC) to record GT sensor outputs and other relevant data during the testing.

7A.4.2.2.3 GT Calibration Results

The sensitivities of all of the GT sensors behaved in the same general way: a 5% rise in the first 500 hours, followed by a gentle decline. The physical reasons for this behavior are not precisely known. It is believed that the long-term decline is caused by the migration of hydrogen atoms from the steel core tube into the fill gas, raising the thermal conductivity and therefore reducing the GT sensitivity. As the migration slows after time, the thermal conductivity stops changing and the GT sensitivity stabilizes.

As for the initial rise in sensitivity, this was not observed in the Limerick test and was not expected. The cause could be a change in the composition or pressure of the fill gas, or it could simply be due to a change in the bypass coolant conditions. Although the physical reason for the initial rise is unknown at this time, the internal calibration system adjusts for the effect.

7A.4.2.2.4 GT Sensitivity Projection

The variation of GT sensitivity can be projected into the future with the simple exponential model. This model works very well after the first 1000 hours. However, it does not explain the initial 5% rise.

The error in projection from one step to the next has been evaluated and the error in the model is very small, normally less than 1%.

7A.4.2.2.5 Steady State Response

Comparison with Neutron TIPs

GT response cannot be compared directly with neutron TIP response. Before a comparison can be made, the GT reading, in millivolts, must be converted into a gamma energy deposition rate, in watts per gram. The gamma energy deposition rate must then be converted into a four-bundle average power distribution, using a suitable gamma detector correlation. Finally, the four-bundle average power distribution must then be converted into an equivalent neutron detector fission rate, using a suitable neutron detector correlation. In this section, and all sections that follow, whenever a GT reading is compared with a neutron detector reading, either TIP or LPRM, it shall be understood that such a transformation has been made.

Eighteen TIP sets were performed in the in-plant test. A comparison of the GT readings with the TIP readings has been made at each set. Since TIP readings have an arbitrary normalization, and are not designed to yield absolute measurements, the GT and TIP readings had to be normalized to the same total value (at each TIP set). This was accomplished by interpolating the TIP readings at the precise GT axial locations, and then summing the results over all of the GTs in this In-Plant test (a total of 18 sensors: 9 in each of 2 strings).

$$\sum_{i=1}^{18} GT_i = \sum_{i=1}^{18} TIP_i$$

The mean value, standard deviation and standard error of the relative differences were calculated for each GT string. The relative differences for RSTK-01 and RSTK-02 ranged between –4.4% to +5.6%. The overall RMS difference was 3.3%.

Comparison with LPRMs

The GT response was compared with the LPRM response. As explained previously, GT response cannot be compared directly with neutron fission detectors, such as LPRMs. Instead, the GT response must be converted to an equivalent neutron detector response. This involves having a detailed knowledge of the surrounding environment: the fuel exposure, water density and especially the control blade positions. This detailed information is available only at those points in time where a TIP set was taken (and a 3D core simulator wrapup file is available).

When the reactor was operating in steady-state at full power, both the GTs and the LPRMs maintained steady, equilibrium values. The LPRM data exhibit significantly more noise than the GT data, in part because it could not be digitally filtered. The data from the Transient Data Recorder, which included the LPRM readings, are available only at one-minute intervals (too slow to filter). The GT data, on the other hand, were available at one second intervals and were filtered with an 8 second filter.

Even the un-filtered GT data however, are less noisy than the LPRM data. There are two physical reasons for this: the first is the thermal mass of the GT sensors, which has the effect of a filter with a relatively long time constant (approximately 18 seconds) and the second is that a significant fraction of the gamma energy comes from delayed gammas. This has a natural smoothing effect.

7A.4.2.2.6 Response During Transients

The observation of the GT response during transient or changing conditions was an important part of the Tokai 2 In-Plant test. As mentioned previously, transient response is not important for the calibration of LPRMs, but it is very important for core monitoring.

One of the factors that limit the transient response of GTs is the effect of delayed gammas. Therefore, a model for delayed gamma compensation was used in this study.

There are four transient response situations which were examined in the In-Plant test: startup, flow change, control blade movement and power down at End-Of-Cycle. Each of these situations is considered separately below.

Response During Startup

The GT and LPRM response for the first two days, April 6th and April 7th, of the startup were reviewed carefully. The LPRMs and their corresponding, adjacent GTs track each other very well. However, the conversion of the GT readings into equivalent fission detector readings requires knowledge of the control blade positions, the void distribution, etc. in the surrounding fuel This information is known most accurately only at the time of the TIP sets. As a result, caution was used in drawing numerical inferences.

Response to Flow Change

The GT response to changes in core flow was studied by carefully analyzing a flow change maneuver that occurred on October 3rd, 1998. This flow change consisted of a gradual reduction in core flow from 100% rated flow to approximately 71% flow over a period of one-half hour. This was in preparation for a control blade adjustment. The rest of this maneuver will be analyzed in the next section on GT response to control blade adjustments.

The percentage differences between the GTs (uncompensated for delayed gammas) and the LPRMs during the flow maneuver are typically 2 to 3% with the largest difference being 3.5%.

One factor that limits the transient response of GTs is the effect of delayed gammas. Although most of the gammas that affect the GTs are in fact prompt and deposit their energy immediately, the delayed gammas are sufficiently numerous to delay the GT transient response. Fortunately, it is possible to compensate for this effect and improve the response. A model for delayed gamma compensation was developed in order to compensate for the time lag in the GT response. In this model, allowance is made for ten groups of delayed gammas, each with its own time constant ranging from a low of 8 seconds to a high of slightly over one day.

The delayed gamma compensation model was applied to the data and in all cases, the time lag was substantially reduced or eliminated entirely. The differences between the GTs and the LPRMs are normally less than 1% with a maximum of 1.8% (one point). This is a very significant improvement over the un-compensated readings.

Response to Control Rod Movement

The GT response to changes in control blade position was studied by analyzing a control blade pattern adjustment that occurred on October 3rd, 1998. This maneuver began with a flow reduction, which was the subject of the previous section. Following the flow reduction, adjustments were made to the control blade pattern and this was followed by an increase in the flow once again.

Although several control blades were moved during the adjustment, there were no blades inserted at any time next to RSTK-01 and the nearest inserted blade was not moved during the adjustment.

In the case of RSTK-02, there was an adjacent control blade that was inserted to notch position 34 at the beginning of the maneuver. At 9:38, it was withdrawn to position 38 and held there until 10:12 when it was inserted to position 34. At 10:16, it was inserted further to position 30, where it remained.

The lag in the GT signals, relative to the LPRMs is evident, both on the way down and on the way back up. As in the previous section, this is explained by the sensitivity of GTs to delayed gammas, which causes their readings to be delayed relative to changes in the fuel fission rate.

The same model for delayed gamma compensation, which was used in the previous section, was applied again to the full control blade maneuver. As before, the thermal time constant of the detectors (which is relatively short) was neglected. In all cases, the time lag was substantially reduced or eliminated entirely.

During the time of the control blade movement, the difference between the un-compensated GT readings and the LPRM readings ranges between -3 % and +4.9 %. The difference in the

delayed gamma compensated readings ranged from -2.7 % up to +4.0 %, not a very large improvement. However, a significant reduction in average difference was made.

Response During Power Down

The GT response to power down at End-of-Cycle was studied by comparison with the LPRM response. The power down began on April 3, 1999 at approximately 18:00 hours. The flow was reduced from 101% rated to 45% rated in the span of about one hour. Further flow reductions and control blade insertions occurred over the next several hours, until 3:00 hours on April 4th. At this point, all rods were inserted and the reactor was shutdown. The recording of the GT response was continued for twelve more hours, in order to gauge the effect of delayed gammas.

As in previous transients, the GT response consistently lags behind the LPRM response. As before, this effect is due to delayed gammas. The application of the delayed gamma compensation model improves the results greatly. In almost all cases, the difference between the GT and LPRM response is less than one-meter unit. This is quite good. However, the compensated GT response does not approach zero as it should. This is most likely due to long half-life (greater than one day) isotopes, which were excluded from the compensation model.

Another way of looking at the GT data is to compare the GT response versus the LPRM response during the power down. The purpose of this is to assess the linearity of the GT response against the LPRM response. As the power drops, uncompensated GT readings drift away from proportionality by several meter units. This is the result of the delayed gammas.

However, after compensation for delayed gammas, the proportionality improves significantly. Similar results were achieved by the seven other GT sensors adjacent to an LPRM. The conclusion is that the GT response, when compensated for delayed gammas, is linear with respect to the LPRM response within one meter unit in the range of power levels from 60 meter units down to zero.

7A.4.2.3 Kashiwazaki-Kariwa 5 In-Plant Test

The Kashiwazaki-Kariwa 5 plant is an 1100 MWe BWR5 operated by Tokyo Electric Power Company. The core has 764 bundles arranged in a “C” lattice configuration. The TIP system is neutron sensitive and has 43 calibration tubes and associated LPRM strings.

The research reported here was sponsored jointly by Tokyo Electric Power Company, Tohoku Electric Power Company, Chubu Electric Power Company, Hokuriku Electric Power Company, The Chugoku Electric Power Company, The Japan Atomic Power Company, Toshiba Corporation, Hitachi, Ltd. and Global Nuclear Fuel – Japan (Reference 7A-3).

7A.4.2.3.1 Test Plan

The test plan was to install 8 LPRM/GT assemblies (4 each from two separate suppliers) into an octant of the core. A comprehensive core monitoring study would therefore be possible, subject only to the condition of octant symmetry. Standard TIP calibration tubes were installed in the LPRM/GT assemblies so that normal TIP set measurements could be taken.

In order to assess the accuracy of core monitoring with GT readings, a bundle gamma scan was to be performed at the end of one cycle of operation. The scan was to include all of the bundles

in the octant of the core as well as three additional bundles chosen so that all four bundles around each LPRM/GT assembly were included.

In addition, comparisons of core monitoring results between the GT and the neutron TIP systems were to be made throughout the cycle.

The LPRM/GT assemblies were to have nine sensors each, arranged in a manner similar to the Tokai 2 In-Plant test.

7A.4.2.3.2 Test Results

The gamma scan measured the strong photo peak of ^{140}La the short-lived daughter of the common fission product ^{140}Ba. Measurements were taken at 17 axial locations, generally every six inches, but excluding nodes obscured by spacers and excluding the top and bottom nodes. The ^{140}Ba distribution was calculated by an off-line core monitoring system throughout the cycle on a time interval of every 3 days. TIP adaptive core monitoring calculations were made 36 times during the cycle for the standard simulation. An equal number of GT adaptive calculations were made for the GT core monitoring simulation. Data were available only for seven of the eight GT assemblies, but this did not significantly detract from the results of the study.

The results showed very good agreement between the calculated and measured ^{140}Ba distributions for both the GT adaptive monitoring and the TIP adaptive monitoring. Table 7A-4 shows the RMS differences between the calculated and measured distributions as measured for the 1D (axial) distribution, for the 2D (bundle) radial distribution and for the 3D (nodal) distribution.

In addition to the gamma scan studies, comparisons were also made between the thermal limits calculated by the two core monitors. The RMS difference for the whole cycle between the MCPR calculated by the GT core monitor and the MCPR calculated by the neutron TIP monitor was 0.008. The maximum difference was 0.02.

Similarly, the RMS difference between the MLHGR calculated by the GT core monitor and the MLHGR calculated by the neutron TIP was 0.4 KW/m and the maximum difference was 1 KW/m.

7A.4.2.3.3 Conclusions

The comparison with the gamma scan established that core monitoring based on GTs is nearly equivalent in accuracy to core monitoring with neutron TIPs. In addition, it was shown that the thermal limits, MCPR and MLHGR, evaluated by the two core monitoring systems were very similar throughout the cycle.

The overall conclusion was that the GT system is “practical as a substitute” for the TIP system.

7A.5 UNCERTAINTY ANALYSIS

7A.5.1 GT Adaptive Core Monitoring Accuracy

Table 7A-5 summarizes the GT core monitoring accuracy criteria and shows the actual values achieved in the core monitoring study. For nodal power uncertainty, the actual result was 3.6% ± 0.2% (two standard error). This means that with a 98% confidence the uncertainty between the

GT and TIP systems is less than 3.8%. This easily meets the 6% criterion. Likewise, the bundle power meets its criterion.

The CPR bias criterion is 2%. This criterion is very tight in consideration of the safety importance of the CPR. The actual value achieved was –1.4% ± 1.4% (two sigma). This means that with 98% confidence the CPR would not be overestimated. The criterion is met.

The LHGR bias criterion is 5%. This criterion is also tight in consideration of the importance of the LHGR in core monitoring. The actual value achieved was 0.5% ± 2.8%. This means that with 98% confidence the LHGR would not be underestimated by more than 2.3%. The criterion is therefore met.

In order to estimate the effect of alternate GT designs involving a fewer number of sensors per assembly, reference is made to calculations involving simulated GT readings. In these calculations, the measured neutron TIP readings were converted to GT readings (using the appropriate gamma and thermal neutron sensor correlations).

The adaptive core monitoring calculations, covering a full cycle, were performed for three different sensor configurations. The first was the standard nine-sensor configuration. The second was a seven-sensor configuration in which the two end sensors were eliminated. The third and final configuration was the minimal configuration of four sensors, one adjacent to each LPRM.

The results as measured by nodal power uncertainty with respect to the neutron TIP cases are shown in Table 7A-6. Since these tests involved simulated, not measured readings, the uncertainties are relatively low. In the final column of the table, the additional uncertainty related to the reduced number of sensors (relative to the standard of nine) is shown.

These additional uncertainties were used to make a more realistic assessment of a real system where the values are measured.

7A.5.2 Estimated Bundle Power Uncertainty

The uncertainty basis for most domestic plants is no longer nodal power uncertainty, but rather bundle power uncertainty. Estimates have been made based on the Tokai 2 In-Plant test. The GT integral update uncertainties were estimated by assuming that the uncertainties for each sensor were uncorrelated with the others. Therefore, the uncertainty for a single sensor was divided by the square root of the number of sensors in a string. The additional bundle power uncertainties are estimated to be zero. The estimated uncertainty for a failed GT heater wire is assumed to be zero, since only one of many strings is affected. Lastly, the uncertainty for a failed GT sensor was estimated to be the same as for an LPRM.

Based on this analysis, the bundle power uncertainty for GT systems is independent of the number of GT sensors and is approximately the same as a TIP system.

Alternatively, the bundle power uncertainty can be based on the Kashiwazaki-Kariwa 5 gamma scan. In this case, the estimated bundle power uncertainty for a GT system is less than for a TIP system, for all sensor configurations.

It is recommended that the former value be used in safety limit analyses, since it is more conservative.

7A.6 CONCLUSIONS

The Gamma Thermometer System has been successfully evaluated as a replacement for the TIP system by a comprehensive In-Plant Test Program. The primary objectives of the Test Program have been met:

(1) GT sensor accuracy relative to gamma TIP, neutron TIP and LPRM measurements has been evaluated; and

(2) GT sensor reliability under BWR operating conditions has been established.

The GT sensitivity trends have been followed throughout a total of three cycles of operation at two BWRs. The sensitivity trend in the most recent test consisted of a relatively rapid initial rise during the first 500 hours of operation, followed by a slow decline for the rest of the cycle.

The GT response in the steady state has been compared with gamma TIP and neutron TIP response as well as the LPRM response. The GT response during changing conditions (startup, flow change, control blade change and power down) has been compared with the LPRM response. Additionally, a GT adaptive core monitoring study has been performed to compare nodal power, CPR and LHGR with corresponding results from neutron TIP adaption.

The GT sensors were evaluated for accuracy with a combination of factory, in-plant and core monitoring tests:

(1) The factory tests proved that the GT sensors met all of the requirements of the SRS.

(2) The in-plant tests proved the accuracy, linearity and range of the GT sensors with respect to the TIPs and LPRMs.

(3) The core monitoring accuracy tests, including nodal power, CPR and LHGR, ascertained GT core monitoring accuracy with respect to neutron TIP monitoring. In addition, core monitoring simulations determined the minimal loss of accuracy in a GT system due to the limited number of readings in the axial direction, as opposed to the nodal data provided by a TIP system.

The overall conclusion of the GT in-plant test program is:

The GT system can be used in place of a TIP system for both LPRM calibration and power shape monitoring.

7A.7 REFERENCES

7A-1 R. H. Leyse, R. D. Smith: “Gamma Thermometer Developments for Light Water Reactors,” IEEE Transactions on Nuclear Science, Vol.N5.26, No. 1, February 1979, pp. 934–943.

7A-2 F. Loisy, M. Huver, M. Janvier: “Technology and Use of Gamma Thermometers,” Specialist Meeting on In-Core Instrument Proceedings, France, June 1988.

7A-3 H. Shiraga, et. al., “Verification of Core Monitoring System with Gamma Thermometer,” International Conference on Global Environment and Advanced Nuclear Power Plants, GENES4/ANP2003, September15-19, 2003, Kyoto, Japan.

Table 7A-1

GT Core Monitoring Component List

Component Name	**Number (Typical)**
LPRM/GT Assembly	64
GT Sensors per Assembly	4
Data Acquisition System Cabinet	2
Heater Power Supplies	8
GT Control Cabinet (including Work-Station)	1

Table 7A-2

Worldwide Experience with Gamma Thermometers

Utility or Company	Unit or Plant	Type GT System	No. Sensors per rod	No. of rods	Year	Comments/Status
DuPont	Savannah River	RPM	N/A	N/A	1950-80	Tritium reactor; GT used for heat flux monitoring. Single point thermocouples used.
OECD Norway	Dodewaard	RPM	1	4	1980	BWR; 10% drift in first two cycles. 1 unit had bad connector failed. Response not stable.
EdF	Bugey-5	RPM	9	2	1979	PWR; no heater this design, 7 of 18 sensors failed. Response not stable.
EdF	Tricastin-3	RPM	9	4	1980	PWR; all sensors working after 4 cycles. Some drift and parasitic noise.
EdF	Tricastin-2	RPM	9	4	1980	PWR; 1 heater failure, heaters not hot enough, 3 sensors failed.
Duke Power Co.	Experimental Unit	N/A	7	1	1982	Irradiated sample tests performed by TEC/ORNL.
EdF	Cruas-2	RPM	9	8	1983	PWR; 18 m long, replaced TIP, after two cycles: within 6% of TIP data, and all sensors working.
SSPB	Forsmark-1	RPM	6	2	1983	BWR; 15 m long, 3 sensor failures during installation only. Operational since 1983.
AP&L	Experimental Unit	RVLMS	9, 14	2	1984	Tested in ORNL loop. 2 GT rods for qualification as RVLMS system.

Table 7A-2

Worldwide Experience with Gamma Thermometers

Utility or Company	Unit or Plant	Type GT System	No. Sensors per rod	No. of rods	Year	Comments/Status
SSPB	Ringhals-2	RPM	9	4	1984	PWR; 35 m long with 9 sensors and 1 heater each. 1 heater failure after 2 cycles.
AP&L	ANO-2	RVLMS	14	2	1985	PWR; operational since 1985; 2 sensors failed.
DuPont	Savannah River	RPM	7	2	1985	Tritium reactor; evaluation units successfully tested.
AP&L	ANO-1	RVLMS	9	2	1986	PWR; in operation since 1986.
General Atomic	Fort St. Vrain	RPM	7	1	1986	GCR; status not known.
SSPB	Ringhals-2	RPM	9	4	1987	PWR; 35 m long with 9 sensors and 1 heater each. No failures in operation.
Consumers Power Co.	Palisades	RVLMS	8	4	1988	PWR; 2 in reactor, 2 spares. 1 sensor failure in 1, 1 sensor & heater in 2nd. Replaced 2nd in 1990. All OK.
Westing-house	Savannah River 1-3	RPM	7	36	1988-89	Tritium reactor; 9 GTs operating OK, 18 more installed & checked out OK, 9 spares.
AP&L	ANO-1	RVLMS	9	4	1990	PWR; 4 spares rods delivered 1990
AP&L	ANO-2	RVLMS	14	4	1990	PWR; 4 spares rods delivered 1991
			———	———		
		Total:	723 sensors	90 rods		

Table 7A-3

Statistical Differences between GT and TIP Readings

	GT 1				GT 2			
	A	**B**	**C**	**D**	**A**	**B**	**C**	**D**
Ave. Err.	3.8%	-1.0%	-2.8%	-3.7%	1.3%	-2.4	-1.6	9.5%
Std. Dev.	2.9%	2.3%	1.5%	1.4%	2.1%	1.1%	0.9%	2.9%
Std. Err.	0.7%	0.5%	0.3%	0.3%	0.5%	0.3%	0.2%	0.7%

Table 7A-4

RMS Differences between Calculated and Measured 140Ba Distributions

Distribution	n TIP vs. γ Scan	GT vs. γ Scan
1D (axial)	1.7%	2.1%
2D (bundle)	2.5%	2.3%
3D (nodal)	3.9%	4.1%

Table 7A-5

GT (9 sensor) Core Monitoring Accuracy Criteria (with respect to n-TIP)

	Description	Target Value	Actual Value (test result)	Meets Req.?
1	GT Nodal Power Uncertainty (σ±2se)	< 6%	3.6%±0.2%⇒3.8%	√
2	GT Bundle Power Uncertainty (σ±2se)	< 4%	1.1%±0.2%⇒1.3%	√
3	GT CPR Bias ± 2σ	< 2%	-1.4%±1.4%⇒0.0%	√
4	GT LHGR Bias ± 2σ	< 5%	0.5%±2.8%⇒-2.3%	√

Table 7A-6

Core Monitoring Nodal Power Uncertainty with Simulated GTs (with respect to n-TIP)

	Description	# of GT Assemblies	# of GTs	Simulated Value ±2se	Additional Unc.
1	Simulated GTs	43	9	2.49%±0.02%	--
2	Simulated GTs	43	7	2.95%±0.02%	1.58%
3	Simulated GTs	43	4	3.56%±0.02%	2.54%

7B. SOFTWARE QUALITY PROGRAM FOR HARDWARE/SOFTWARE DESIGN AND DEVELOPMENT

Reg. Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," which endorses IEEE Std 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," provides guidance for complying with requirements for safety systems that use digital computer systems (see Reference 7B-1 and 7B-2). Branch Technical Position HICB-14 (BTP-14) outlines the many activities to be considered when constructing a software development program for software-based control and instrumentation (C&I) system, herein refers to as software-based product (see Reference 7B-3). BTP-14 divides these activities into 11 separate software development plans. The overall requirement is that the essential elements of each of the 11 development groups are addressed and documented. GE has developed and accumulated the experiences and documentation of various aspects of the software development plans called out in BTP-14, in GE's design work of software-based products in current products including that of advanced reactor. The ESBWR software development program will be developed using GE's current software development plans as bases. The ESBWR software life cycle process planning documents as reflected in Section 2.1 of BTP 7-14 will be developed and submitted to NRC for review in support of the DCD Certification. The development of the plans will address various aspects of the software development and quality addressed in the guidance documents of various related industry standards and regulatory guides. In certain cases, deviation may be taken from the detailed requirements described in those guidance documents, whereas the process outlined in this appendix will be followed. This appendix summarizes the development activities to be implemented for ESBWR safety-related software-based products with documentations in the following subject areas:

- Software Quality Assurance Plan
- Software Management Plan
- Software Development Project plan
- Software Configuration Management Plan
- Software Verification and Validation Plan
- Software Safety Plan (SSP)
- Software Test Plan (SVTP)
- Training Plan
- Operations and Maintenance Plans
- Integration Plan
- Installation Plan

The following paragraphs summarize that through these above development work how the ESBWR safety-related software development process intends to meet the requirements of BTP-14.

7B.1 SOFTWARE QUALITY ASSURANCE PROGRAM

The Software Quality Assurance Program (SQAP) outlined below describes a systematic approach to the development and use to be implemented for ESBWR software development. It also identifies the documentation to be prepared during the software development, verification, validation, use, and maintenance (see Reference 7B-4). It is conformed to the requirements of 10 CFR 50, Appendix B and is consistent with the requirements specified in IEEE-730, "IEEE Standard for Quality Assurance Plans." (See Reference 7B-5.) This outline in conjunction with other plans described in this appendix addresses the various elements described in the related guidance documents including IEEE-730.

(1) The SQAP: Defines the quality assurance management of the software-based product. This includes:

   a. The organizational structure that influences and controls the quality of the software. The SQA organization shall maintain independence from the development organization.

      The organizational boundaries between the software QA organization and other company organizations.

   b. The responsibilities and authority of the software quality organization, and identify the specific organizational elements responsible for each task (i.e., configuration management, V&V, safety analysis, etc)

   c. Tasks to be performed with special emphasis on software quality assurance activities for each software life cycle phase (described in the Software Management Plan)

(2) Defines the documentation governing the development, verification and validation, use, and maintenance of the software-based product and state how each documents are to be checked for adequacy, and the documentation needed to ensure that the implementation of the software satisfies requirements.

(3) Defines the standards, practices, conventions and metrics to be applied and how compliance with these requirements is to be monitored, and assured traceability is maintained through all phases of the software life cycle.

(4) Defines the reviews and audits to be conducted and accomplished, such as (but not limited to), software requirements review, software design review, managerial reviews, functional audits and in-process audits; and if applicable, defines further actions required and how they are to be implemented and verified

(5) Describes the practices and procedures to be followed for reporting, tracking, and resolving problems identified in both software items and the software development and maintenance process.

(6) Identifies the special software tools, techniques, and methodologies that support SQA.

(7) Defines the methods use to control and secure the software source code and software media.

(8) Defines the provisions for assuring that software provided by suppliers through purchase meet the established requirements; also for assuring SQAP covers the proper methods used

to assure the suitability of previously-developed software for use with the software-based product.

(9) Identifies the SQA documentation to be retained, the methods and facilities to be used to assemble, safeguard, and maintain this documentation, and the retention period.

7B.2 SOFTWARE MANAGEMENT PLAN

The Software Management Plan (SMP) outlined below describes the management of the software development in accordance with Reg. Guide 1.173, "Development Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants". (See Reference 7B-6.) This outline in conjunction with other plans described in this appendix addresses the various elements described in the related guidance documents including Reg. Guide 1.173. The SMP defines:

(1) The Organizational Structure describing the boundaries, interfaces and responsibilities for development of the software design.

(2) The Management activities in:

a. Software developed by subcontractors;

b. Procedures to be used in the software development; the interrelationships between software design activities;

c. Security to provide assurance that the integrity of the software-based product is maintained, and to provide methods to be used to prevent contamination of the developed software by viruses;

d. Adaptation of previously developed software;

e. Use of commercial off-the-shelf software (COTS) (see References 7B-7 and 7B-8);

f. System for collection of software metrics and using them to improve processes and software quality.

(3) The software engineering process, which is composed of the following life-cycle phases:

a. The Planning Phase. The planning phase design activities address the following system design requirements and software development plans and review report:

(i) Software Management Plan

(ii) Software Development Project Plan

(iii) Software Configuration Management Plan

(iv) Verification and Validation Plan

(v) Equipment design requirements

(vi) Disposition of design and/or documentation of non-conformances identified during this phase

b. The Design Definition (Requirements) Phase. Design Definition (Requirements) Phase design activities address the development of the following equipment design and configuration requirements in accordance with Reg. Guide 1.172, "Software

Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." The design and review activities are documented in the following documents and drawings, analysis and review reports:

(i) System Requirements Specification

(ii) Equipment schematic

(iii) Equipment hardware and software performance specification

(iv) Equipment user's manual (Operation and Maintenance Manual)

(v) Data communications protocol

(vi) Safety analysis of the developed design definition

(vii) Disposition of design and/or documentation of non-conformances identified during this phase.

c. The Software Design phase. The Software Design phase addresses the design of the software architecture and program structure elements, and the definition of software module functions. The design and review activities are documented in the following documents, analysis and review reports:

(i) Software Design Specification

(ii) Safety analysis of the software design

(iii) Disposition of design and/or documentation of non-conformances identified during this phase.

d. The Software Coding phase. The Software Coding phase activities address the implementation and testing of software design. The implementation and review activities are documented in the following documents, analysis and review reports:

(i) Software source code listings

(ii) Software module test reports

(iii) Safety analysis of the software coding

(iv) Disposition of non-conformances identified in this phase's design documentation and test results.

e. The Integration Test Phase. Integration test phase describes the integration process and addresses the equipment testing activities that evaluate the performance of the software being installed in prototype hardware. The installation shall be performed in accordance with defined methods and procedures. The test and review activities are documented in the following analysis and review reports:

(i) Installation and Integration test reports

(ii) Safety analysis of the integration test results

(iii) Disposition of non-conformances identified in this phase's design documentation and test results.

f. The Validation Test Phase. Validation test phase activities address the V&V testing activities that demonstrate that the software-based product is operational and conforms to all functional and performance requirements as defined in the Design Definition phase. The test and review activities are documented in the following analysis and review reports:

(i) Validation test plans and procedures

(ii) Validation test reports

(iii) Description of as-tested software

(iv) Safety analysis of the validation test results

(v) Disposition of non-conformances identified in this phase's design documentation and test results

g. The Change Control Phase. The Change Control phase begins with the completion of validation testing. It provides a controlled path through the design process (operation) that may be invoked when software modification is required.

7B.3 SOFTWARE DEVELOPMENT PROJECT PLAN

Software Development Project Plans outlined below define the managerial processes necessary to accomplish the design and development of the ESBWR software-based products. Software Development Project Plans are developed as a supplemental document to the SMP. This outline in conjunction with other plans described in this appendix addresses the various elements described in the related guidance documents including IEEE-1058.1 (see Reference 7B-9). Software Development Project Plans are used as a tool to aid, as a minimum, the following project management activities and as such may be updated throughout the course of the project:

(1) Establish the project goals, deliverables and principle work packages;

(2) Establish schedules and milestones for each project deliverable and work package;

(3) Coordinate between ESBWR project team and interfacing organizations including subcontractors responsible for software development;

(4) Develop constraints and mechanism to track and report progress;

(5) Establish plans of resources and staffing, qualifications, and training of project personnel;

(6) Establish description of the methods, techniques, and tools used;

Software Development Project Plans uses the format specified in IEEE 1058.1, "Standard for Software Project Management Plans."

7B.4 SOFTWARE CONFIGURATION MANAGEMENT PLAN

The Software Configuration Management Plan (SCMP) outlined below defines the specific product or system scope to which it is applicable, the organizational responsibilities for software configuration management, and methods to be applied to. This outline in conjunction with other plans described in this appendix addresses the various elements described in the related guidance documents including Reg. Guide 1.169, "Configuration Management Plans for Digital Computer

Software Used in Safety Systems of Nuclear Power Plants." (See References 7B-10, 7B-11 and 7B-12.) The SCMP provides:

(1) Description of the SCM organization, which includes the description of responsibilities of each individual for carrying out each SCM activity, identifies the individual with authority to authorize release of any software, data, or document for revision.

(2) A list of documents to be placed under configuration control.

(3) SCM activities, which include

a. Process to manage changes to design interface documentation and software design documentation;

b. Designate and control software revision status. Such methods shall require that software code listings present direct indication of the software code revision status;

c. Baseline reviews of the software development process to be conducted during each phase of the software development life cycle, and the scope and methods to be used in the baseline reviews to evaluate the implemented design, design documentation, and compliance with the requirements of the Software Management Plan and Configuration Management Plan;

d. Configuration management of tools (such as compilers) and software development procedures;

e. Configuration review and audits;

f. Control of vendor(s) responsible for software development;

g. Methods for error tracking and analysis of failures during software development, such as the use of software metrics;

h. Evaluate and track commercial off-the-shelf (COTS) software in accordance with EPRI TR-106439 (Reference 7B-7) and CR-G421 (Reference 7B-8), "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications", and method of tracking tool history and errors.

(4) Description of the procedures to be used in configuration management, as a minimum, includes:

a. Naming conventions and procedures for placing items under configuration control;

b. Procedures for managing software libraries;

c. Procedures to manage the change process, reporting procedures, change approval procedures;

d. Procedures for maintaining status of design interface documentation and developed software design documentation, change histories, backup and recovery;

e. Tracking and synchronization procedures, and procedures for protecting configuration management records, including controlling source and object code during and after the project development process;

f. Procedures for managing corrective actions to resolve deviations identified in software design and design documentation, including notification to end user of errors discovered in software development tools or other software;

g. Methods for design record collection and retention;

h. Methods for tracking error rates during software development, such as the use of software metrics and actions taken on recommendations to improve operation.

7B.5 VERIFICATION AND VALIDATION PLAN

The Verification and Validation Plans (V&VP) outlined below define the verification and validation process to assure the following (see Reference 7B-13):

(1) V&V shall be performed as a controlled and documented evaluation of the conformity of the developed design to the documented design requirements at each phase of baseline review;

(2) Software outputs of each life cycle phase are in compliance with the requirements defined in the previous phase;

(3) Final software product meets the system requirements and applicable established standards.

The Verification and Validation Plans, in conjunction with other plans described in this appendix address the various elements and are intended to meet the requirements specified in Reg. Guide 1.168, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems for Nuclear Power." (See Reference 7B-14.) It provides:

(1) Description of the organization supporting the software V&V effort. This includes:

a. V&V staff qualification and responsibilities of individual carrying out each V&V task and personnel assignments for performing the V&V tasks;

b. Approval authority reporting channels;

c. Organizational interfaces;

d. Training requirements.

(2) Description of the degree of independence between the development team and independent V&V Team.

(3) Description of how the V&V effort will be managed. This includes

a. Reporting procedures;

b. Management reviews and audits. Design verification reviews shall be conducted as part of the baseline reviews of the design material developed during the Planning through Integration phases of the software development life-cycle, and that validation testing shall be conducted as part of the baseline review of the Validation phase of the software development life-cycle;

c. Methods of carrying out the different V&V activities, and validation testing shall be conducted per documented test plan and procedure;

d. Completion criteria for the V&V activities. Software development is not complete until the specified verification and validation activities are complete and design documentation is consistent with the developed software;

e. Evaluation of commercial software and commercial development tools for safety-related applications;

f. V&V requirements for non-conformance tracking and closure.

Schedule, milestone and resources plans needed to support the V&V activities.

(6) A description of the V&V activities, including

a. Verification and Validation Methods and Test Tool;

b. Acceptance criteria for each activity;

c. Relationships with the product development life cycle tasks;

d. Coordination with SCM activities.

(7) Description of all required testing and test documentation requirements, including error reporting and methods for identification, closure, and documentation of design and/or design documentation non-conformances and anomaly resolution procedures.

(8) Description of V&V documentation and reporting requirements, including:

a. The individual and/or team conducting the V&V;

b. Activities during the V&V, including the V&V inputs and outputs, traceability matrix (forward and backward direction), evaluation criteria and non-conformances identified during the V&V. The products which shall result from the baseline reviews conducted at each phase of the software development life cycle; and that the defined products of the baseline reviews and the V&V Plan shall be documented and maintained under configuration management;

c. Use of commercial software and commercial development tools for safety-related applications is a controlled and documented procedure.

7B.6 SOFTWARE SAFETY PLAN

This Software Safety Plan (SSP) outlined below establishes the processes and activities intended to be used to ensure the safety of the safety related software for the software-based product and to address the potential software risks. This outline in conjunction with other plans described in this appendix addresses the various elements described in the related guidance documents including the guidelines described in IEEE 1228, "Software Safety Plans." (See Reference 7B-15.) The Software Safety Plan exhibits the following characteristics:

(1) Specify the purpose and scope of the software safety activities.

(2) Define the responsibilities and authority of the software safety organization (i.e., specify a person or group responsible for software safety tasks). The designated individual shall have a clear authority for enforcing safety requirements in the software-based products being designed and developed. The software safety organization shall have the authority to

reject the software, including previously developed software, support software and third party software if the software cannot be shown to be adequately safe.

(3) Plan the resources required for the software safety organization, including qualification and training requirements.

(4) Describe the management of software safety activities, including how the safety activities are integrated and coordinated between the development team and other organizations (i.e., software safety organizations, Quality Assurance, Configuration Control Management, vendors).

(5) Describe the safety analyses to be performed and documented on each of the principle design documents for software life cycle phases defined in the Software Management Plan.

(6) Describe the documentation requirements for software safety analysis, including configuration management of the software safety documents.

(7) Describe any safety related tests that are not included in the Software Verification and Validation Plan.

7B.7 SOFTWARE TEST PLAN

The Software Test Plan outlined below describes the software test activities to be carried out during the development process of software-based product. This test plan outline, in conjunction with other plans described in this appendix, addresses and is intended to meet the requirements specified in Reg. Guide 1.170, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants" (Reference 7B-16), and Reg. Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." (Reference 7B-17.) The test plan exhibits the following characteristics:

(1) Description of the test organization, which includes the description of responsibilities of each individual for carrying out each test activity;

(2) Description of test management, such as (but not limited to) schedule, resources, security, risks and contingency planning, anomaly and problem reporting, and training needs;

(3) Description of the scope of the equipment to be tested;

(4) Definition of Software Test Guidelines for:

a. Test preparation to assure that the required test activities can be properly carried out within the project schedule. This is accomplished by identification of resources, including applicable tools and environmental conditions required to support the development, execution, and the documentation of the test.

b. Test design to specify the test strategies (acceptance criteria, test techniques and test approaches) to assure completeness of the test coverage.

c. Test execution to analyze the test item in order to evaluate each identified feature or combination of features to determine if the feature or combination of features are passed or failed based on the defined acceptance limits.

d. Test summary to summarize the results of the designated testing activities and to provide evaluations based on these results.

(5) Definition of test methods such as:

a. Module (unit) testing. Module testing is the verification of the internal structure of individual software modules, or a group of modules, to ensure that each software function allocated in the Software Design Specification (SDS) performs as intended.

b. Integration testing. Integration testing is an orderly progression of testing to uncover errors associated with software and hardware interfaces. Integration testing is performed to verify that all software modules perform as intended and conform to requirements (such as but not limited to interfaces, stress, security, and self test) after being installed in the hardware. System validation testing. System validation testing relies entirely on black-box testing techniques and is executed using formally prepared test procedures to assure the system is operational and conforms to all functional and performance requirements specified in the System Requirements Specification (SRS).

(6) Definition of all required test documentation, such as testing plans, specifications, procedures and cases, and summary and anomaly reports.

(7) Measurement system for error tracking and resolution, and to assess the success or failure of the test effort.

7B.8 OPERATIONAL AND MAINTENANCE PLANS (O&M MANUAL)

This is the Software Operations Plan and Software Maintenance Plan. The O&M Manual outlined below, which complies with the software maintenance guidelines specified in IEEE Std. 828, "IEEE Standard for Software Configuration Management Plans", and IEEE Std. 1042, "IEEE Guide to Software Configuration Management", will be established for software-based products.

The O&M Manual describes the instruction and guideline to operate and maintain the software-based product. The O&M Manual exhibits the following characteristics:

(1) Describes the organization supporting the software-based product operations and maintenance effort. This includes:

a. The qualification and responsibilities of individual carrying out each operations and maintenance task;

b. Personnel assignments for performing the operations and maintenance tasks;

c. Security measures to limit access to information, use of critical functions, and changes to critical functions;

d. Organizational interfaces;

e. Training requirements.

(2) Define the procedures to allow responsible personnel to:

a. Initiate and perform normal system operational activities;

b. Perform required maintenance and perform troubleshooting when abnormal conditions for system operation occur;

c. Develop problem reporting channel, and for resolution of those problem reports.

(3) Specify the methods, techniques and tools use to accomplish the maintenance function.

(4) Include the required system documentation such as (but not limited to) elementary diagram, schematic, system guides to assist operations and maintenance personnel in operating and maintaining the software-based product.

(5) Define the procedures on failure detection during operation, correction of faults that have caused those failures, and if applicable, regression testing to be conducted.

(6) Define procedures to shut down and restore the software-based product to normal operation.

(7) Provide a list of recommended spare parts so that an appropriate site plan can be implemented for obtaining spare parts and performing replacement if needed to assure continued, reliable and safe operation.

(8) Develop a system for collection of metrics and using them to assess the success or failure of the operating and maintenance procedures.

7B.9 TRAINING PLAN

The training plan outlined below describes the management, implementation, and resource characteristics of the training program. The training plan defines:

(1) Description of the organization supporting the software-based product training effort. This includes:

(2) Organizational interfaces and responsibilities; the qualification and responsibilities of individual carrying out each training module and personnel assignments for performing the training. The qualified trainers must be knowledgeable in the operation of software-based product.

(3) Overall objectives, describing the training needs of appropriate plant staff, including operators and I&C engineers and technicians.

(4) The methods, techniques, tools and facility use to accomplish the training function.

(5) Written test or assessment that demonstrates the student's knowledge as it relates to the objectives. This covers test and/or quiz that relates directly to the subject material presented to the student.

7B.10 INTEGRATION PLAN

The integration plan outlined below summarizes the management, implementation, and resource characteristics of the integration program.

(1) Description of the purpose, organization, and responsibilities.

   a. Description of the software integration process and the hardware/software integration process; and

   b. Description of the software integration organization, including the boundaries between the software integration organization and other company organizations, as well as reporting channels

(2) Description of the measurement and procedures.

a. Description of measurement of the implementation of the integration effort. Description of data collection and analysis associated with the integration of the software and of the hardware/software combination, to determine the adequacy of the integration effort.

b. Description of procedures, methods, and controls for software integration and combined hardware/software integration. This includes the design outputs and reports, and documentation describing the software integration tests and the hardware/software integration tests.

(3) Description of the methods and tools.

a. Description of the qualification of the integration tools appropriate to the safety significance of the software, which is to be created using the tools.

7B.11 INSTALLATION PLAN

The installation plan outlined below summarizes the management, implementation, and resource characteristics of the installation program.

(1) Description of purpose, organization and responsibilities.

a. Description of the installation process, the goals of that process, as well as the environmental conditions within which the computer system and software system is qualified to operate. Description of the software installation organization, including such as the boundaries between the software installation organization and the broader safety system installation organization.

c. Description of the responsibilities and authority of the software installation organization.

(2) Description of measurement and procedures.

a. Description of the measurement implementation of the installation effort, including installation data collection and analysis.

b. Description of procedures, methods, and controls for software installation and combined hardware/software installation. This includes checking procedures for proper computer system and sensors/actuators functionality, installation of correct software version, installation anomalies, testing, etc.

(3) Description of methods and tools.

a. Description of the methods, techniques and tools to be used to accomplish the installation function, as well as the qualification of the tools appropriate to the safety significance of the software, which is to be installed using the tools.

7B.12 REFERENCES

7B-1 USNRC, “Criteria for Digital Computers in Safety Systems of Nuclear Power Plants,” Reg. Guide 1.152.

7B-2 IEEE Std. 7-4.3.2, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."

7B-3 USNRC, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," Branch Technical Position HICB-14.

7B-4 GE Energy Nuclear, "ESBWR I&C Software Quality Assurance Plan," NEDO-33245, Class I (Non-proprietary), January 2006.

7B-5 IEEE-730, "IEEE Standard for Quality Assurance Plans."

7B-6 USNRC, "Development Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.173.

7B-7 Electric Power Research Institute, "Guidelines on Evaluation and Acceptance of Commercial Grade Digital Equipment in Nuclear Safety Application," EPRI TR-106439.

7B-8 CR-G421, "A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications."

7B-9 IEEE 1058.1, "Standard for Software Project Management Plans."

7B-10 USNRC, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.169.

7B-11 IEEE Std. 828, "IEEE Standard for Software Configuration Management Plans."

7B-12 IEEE Std. 1042, "IEEE Guide to Software Configuration Management."

7B-13 GE Energy Nuclear, "ESBWR I&C Software Verification and Validation Plan," NEDO-33228, Class I (Non-proprietary), January 2006.

7B-14 USNRC, "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems for Nuclear Power," Reg. Guide 1.168.

7B-15 IEEE 1228, "Software Safety Plans."

7B-16 USNRC, "Software Test Documentation for Digital Computer Software used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.170.

7B-17 USNRC, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," Reg. Guide 1.171.